Graupner, Dustin

Konzeption und Umsetzung eines Komplexpraktikums zur Netzwerksimulation unter Verwendung der Cisco Software Packet Tracer

DIPLOMARBEIT

Fakultät Medien

Fachbereich Netzwerktechnik und Administration

Mittweida, 2016

Graupner, Dustin

Konzeption und Umsetzung eines Komplexpraktikums zur Netzwerksimulation unter Verwendung der Cisco Software Packet Tracer

eingereicht als

DIPLOMARBEIT

an der

HOCHSCHULE MITTWEIDA (FH)

UNIVERSITY OF APPLIED SCIENCES

Fakultät Medien

Fachbereich Netzwerktechnik und Administration

Mittweida, 2016

Erstprüfer: Prof. Dr.-Ing. Frank Zimmer

Zweitprüfer: Dipl.-Ing. (FH), M. Sc. Rico Thomanek

Vorgelegte Arbeit wurde eingereicht am: 21.01.2016

Bibliografische Beschreibung

Graupner, Dustin:

Konzeption und Umsetzung eines Komplexpraktikums zur Netzwerksimulation unter Verwendung der Cisco Software Packet Tracer

Hochschule Mittweida (FH), Fakultät Medien, Fachbereich Netzwerktechnik und Administration

Referat:

Diese Diplomarbeit behandelt die Thematik der Netzwerktechnik und die softwarebasierte Simulation von Netzwerken. Im Rahmen dessen wird das von Cisco entwickelte Programm Packet Tracer vorgestellt und unter Zuhilfenahme dieser Software ein Praktikum entwickelt, welches zur Lehre in der Kommunikationstechnik eingesetzt wird.

Vorwort

Diese Diplomarbeit wurde im Wintersemester 2015/2016 an der Hochschule Mittweida angefertigt.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. Frank Zimmer, sowie Herrn Dipl.-Ing. (FH), M. Sc. Rico Thomanek für die fachliche und mentale Unterstützung während der Bearbeitung.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

A

ARP Address Resolution Protokoll

C

CLI Command Line Interface

CSMA/CD Carrier Sense Multiple Access/Collision Detection

D

DCE Data Circuit-Terminating Equipment

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DTE Data Terminal Equipment

H

HTTP Hyper Text Transfer Protocol

I

ICMP Internet Control Message Protocol

IMAP Internet Message Access Protocol

IOS Internetwork Operating System Software

IP Internet Protocol

L

LAN Local Area Network

M

MAN Metropolitan Area Network

N

NAT Network Address Translation

NAPT Network Address Port Translation

O

OSI Open Systems Interconnection (Model)

P

PC Personal Computer

Ping Packet Internet Groper

POP3 Post Office Protocol (Version 3)

S

SMTP Simple Mail Transfer Protocol

U

USB Universal Serial Bus

V

VLAN Virtual Local Area Network

W

WAN Wide Area Network

WLAN Wireless Local Area Network

1 Einleitung

1.1 Motivation

Als das Internet in den frühen Neunziger Jahren seinen kommerziellen Einzug hielt, war vermutlich niemandem bewusst, dass es eines Tages nahezu alleinig den weltweit gesamten Informationsaustausch kontrollieren würde. Die globale Vernetzung hat seitdem nie aufgehört, sich weiter zu entwickeln. Ununterbrochene Verbindung mit dem Internet, Fahrzeuge, welche eigenständig aktuelle Stauinformationen ermitteln und Kleidung, welche die Körperfunktionen ihres Trägers überwacht werden in naher Zukunft zur alltäglichen Normalität gehören. Mit dem Aufkommen neuer Technologien, wie Smart Home oder dem Internet der Dinge und die damit verbundene komplette Vernetzung der Welt wird das Gebiet der Netzwerktechnik auf eine neue Stufe gehoben und macht diese damit zu einer immer wichtiger werdenden Thematik.

1.2 Zielstellung

Kernziel dieser Diplomarbeit ist die Entwicklung eines Komplexpraktikums, welches Studenten[1] der Medien- und Kommunikationstechnik in das Gebiet der Netzwerktechnik einführt und grundlegende Kenntnisse über verschiedene Technologien vermittelt. Parallel dazu wird ein Einblick in existierende, im Rahmen des Praktikums verwendete Netzwerktechnologien gegeben und die Thematik der Netzwerksimulation behandelt. Zusätzlich dient diese Arbeit als Nachschlagewerk für Anwender, welche das entwickelte Praktikum absolvieren, einschließlich der Aufschlüsselung der einzelnen Versuche und Lösungsansätze zu diesen. Die verwendete Netzwerksimulationssoftware Cisco Packet Tracer wird dabei ebenfalls

[1] Um den Lesefluss nicht zu beeinträchtigen, wird auf eine Unterscheidung der männlichen und weiblichen Schreibweise, wie z.B. Studenten und Studentinnen, verzichtet. Die männliche Form wird neutral und ohne Wertung verwendet. Falls ausschließlich das weibliche Geschlecht gemeint ist, wird diese Form explizit benutzt.

näher analysiert. Es schließt sich eine Einführung in die elementaren Funktionen des Programmes an, um den Bearbeiter des Praktikums mit dessen Handhabung vertraut zu machen.

1.3 Kapitelübersicht

Die vorliegende Diplomarbeit wird in folgende Kapitel unterteilt:

Kapitel 1 führt in die Thematik dieser Diplomarbeit ein und beinhaltet deren Zielstellung und Motivation. Des Weiteren wird eine Übersicht über die einzelnen Kapitel gegeben.

Kapitel 2 gibt einen Überblick über die Thematik der Netzwerksimulation. In diesem Abschnitt wird näher auf die Einsatzgebiete, sowie die Gründe für die Verwendung von Netzwerksimulationssoftware eingegangen. Abschließend für dieses Kapitel folgt eine Gegenüberstellung zweier Softwarebeispiele aus diesem Bereich.

Kapitel 3 beschäftigt sich mit der von der Cisco Systems Inc. entwickelten Netzwerksimulationssoftware Packet Tracer, welches als Grundlage für das in der Arbeit abgehandelte Praktikum dient. Es werden Funktionsweisen, Möglichkeiten, sowie unterstützte Hardware näher betrachtet. Außerdem wird in einem kurzen Exkurs auf wichtige Befehle und Funktionsweisen der Kommandozeile eingegangen, welche zur Konfiguration von Cisco Hardware verwendet wird.

Kapitel 4 geht auf den Kern der Diplomarbeit ein, welche die erarbeiteten Praktika bilden. Es setzt sich mit dem methodischen Aufbau der einzelnen Versuche auseinander und behandelt verwendete Technologien, welche den Studierenden mit Hilfe der Versuche nähergebracht werden. Basierend auf jedem einzelnen Versuch werden auch Lösungsmuster gestellt.

Kapitel 5 bildet den Abschluss dieser Facharbeit. Darin werden Erkenntnisse und gewonnene Erfahrungen, resultierend aus der Bearbeitung der Aufgabenstellung vorgestellt. Abschließend wird auf Erweiterungsmöglichkeiten der Praktika eingegangen, auf Grundlage der Resonanz der Seminargruppen, in welchen das Praktikum erstmalig zum Einsatz kam.

2 Netzwerksimulation

2.1 Einsatzgebiete und Gründe der Netzwerksimulation

2.1.1 Lehre

Die Simulation von Netzwerkumgebungen kann in zahlreichen Bereichen von Nutzen sein. Die häufigste Anwendung findet sich dabei in der Lehre. Netzwerksimulation wird in diesem Feld eingesetzt, um Lernenden ein Verständnis für verschiedene Netzwerktechnologien zu vermitteln und ihnen die Funktionsweise und den Aufbau von kleinen und großen Netzwerken näher zu bringen, ohne große Investitionen in Neuanschaffungen von Netzwerkequipment zu tätigen. Durch die grafische Darstellung können Prozesse und Protokollverwendungen veranschaulicht werden, was einen tieferen Einblick in die Thematik gewährt und damit das reine theoretische Studieren von Netzwerkgrundlagen positiv unterstützt. Weiterhin wird es so möglich, den Umgang mit Netzwerkkomponenten zu erlernen, zu welchen eine bestimmte Bildungseinrichtung beispielsweise keinen Zugang hat. Damit haben Studierende größere Möglichkeiten und können sich in weitaus größerem Umfang mit dem Thema auseinandersetzen. Dass sich die Verwendung solcher Software im Lehrsektor durchsetzt, zeigt zum Beispiel die Cisco Networking Academy, welche das Programm Packet Tracer in den Kursen für deren CCNA und CCNP-Zertifikate[2] mit Erfolg einsetzt.

2.1.2 Unternehmen

Auch für Unternehmen kann der Einsatz von Netzwerksimulationssoftware interessant sein. An dieser Stelle ist besonders der monetäre Aspekt erwähnenswert. Eine genaue Simulation vor Anschaffung des Firmennetzwerks kann dabei helfen, Kosten für eventuelle Fehlkäufe zu sparen oder mögliche Fehler

[2] Vgl. [Web01]

in der Netzwerkplanung aufzuzeigen. Außerdem verschafft es einen Überblick, welche und wie viele Komponenten im geplanten Projekt zum Einsatz kommen sollen. Eine strukturierte Planung unter Zuhilfenahme einer Simulationssoftware kann ebenfalls dazu beitragen, eventuelle Sicherheitslücken im geplanten Netzwerk festzustellen und dementsprechende Änderungen vorzunehmen. Soll ein bereits bestehendes Netzwerk ausgebaut werden, können Anpassungen zunächst mit Hilfe einer Simulationssoftware implementiert und auf Kompatibilität überprüft werden. Zudem ist es möglich, mit einem solchen Programm eine Fehleranalyse durchzuführen, um schwache Glieder im Firmennetzwerk zu eruieren und gegebenenfalls zu ersetzen oder bei Neueinrichtung jenen Fehlern vorzubeugen.

2.1.3 Privatanwender

In Privathaushalten finden Netzwerksimulatoren vergleichsweise wenig Anwendung. Jedoch sind diese auch im Heimsektor vielseitig einsetzbar. Smart Home beispielsweise findet immer häufiger Anwendung und ist für viele Haushalte mittlerweile erschwinglich. Gerade bei Neubauten ist es zunehmend von Bedeutung, den Haushalt netzwerkfähig zu gestalten. Beim Design eines Heimnetzwerkes kann die Verwendung einer Simulationssoftware durchaus von Vorteil sein und den Nutzer vor Kosten eines oder mehrerer Fehlkäufe bewahren.

2.2 Gegenüberstellung ausgewählter Software

Unter diesem Punkt erfolgt eine Gegenüberstellung aktueller Softwarebeispiele. Dabei wird Cisco Packet Tracer, auf welchem diese Arbeit aufbaut, mit der Software Graphical Network Simulator-3 (GNS-3) und dem gängigen Simulationsprogramm Boson NetSim verglichen. Dabei werden sowohl Einsatzmöglichkeiten, Kosten, Handhabung, sowie der Aufbau der Software analysiert. Ziel dieses Punktes ist es, einen kurzen Überblick über verschiedene, am Markt vertretene Programme zu ermöglichen und abschließend aufzuzeigen, aus welchen Gründen die Software Packet Tracer für ein einführendes Praktikum, wie es im Rahmen dieser Arbeit entwickelt wurde, am besten geeignet ist. Wenn nicht anders angegeben, handelt es sich bei dieser Gegenüberstellung um Erfahrungswerte, welche sich durch Tests der jeweiligen Software entwickelt haben.

Zunächst wird sich mit dem Aufbau und der Bedienung der Programme beschäftigt. Die Programme verfügen alle über eine grafische Oberfläche, wodurch sich das Arbeiten anschaulich gestalten lässt. Ebenfalls fällt die Bedienung der Programme ähnlich aus, alle arbeiten nach dem Prinzip, verschiedene Netzwerkkomponenten auf einer Arbeitsfläche zu vernetzen und das erstellte Netzwerk zu analysieren und zu testen. Während jedoch Packet Tracer und GNS-3 vergleichsweise übersichtlich erscheinen, wirkt die Oberfläche von NetSim verhältnismäßig komplex, was folgende Abbildungen aufzeigen (Abbildungen 2.1, 2.2, 2.3).

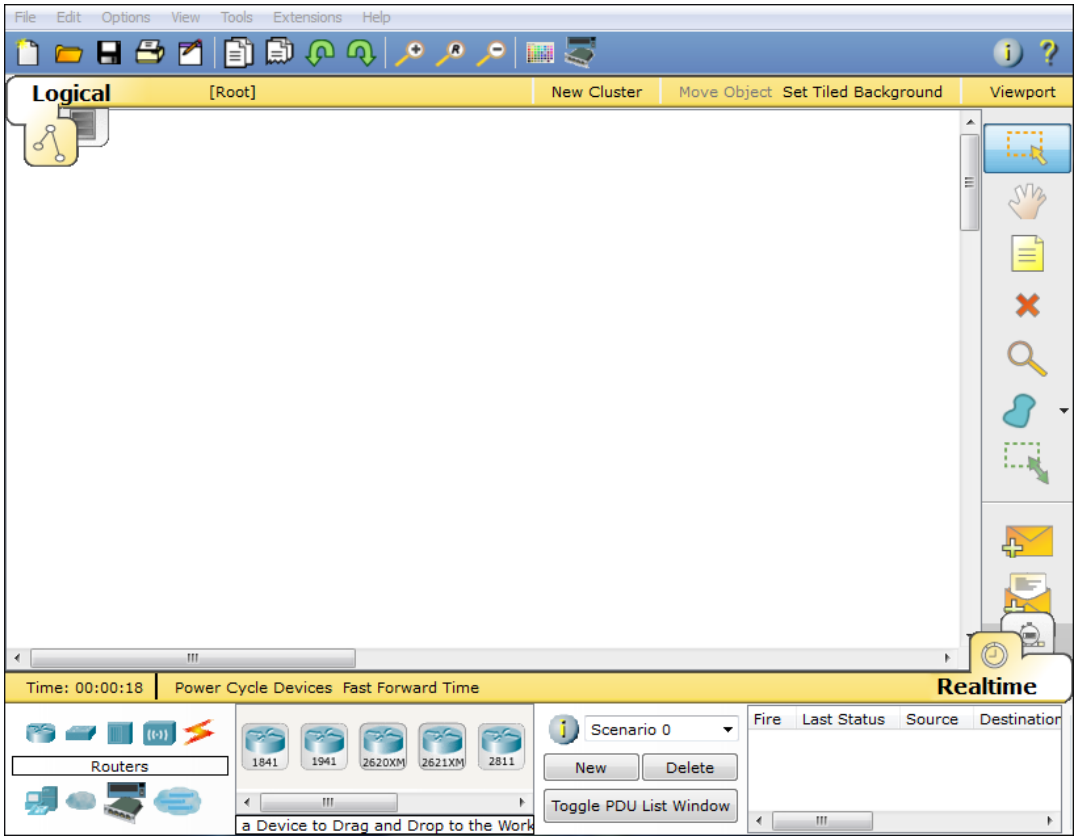

Abbildung 2.1, Oberfläche Packet Tracer

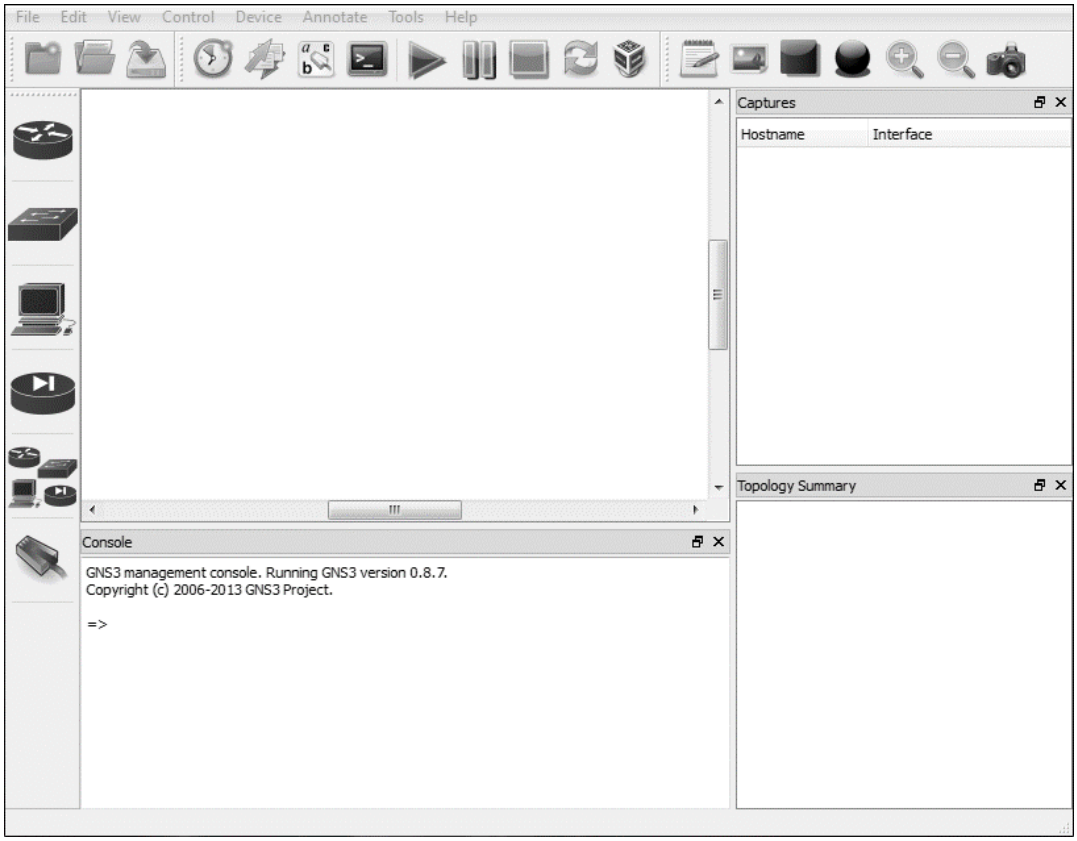

Abbildung 2.2, Oberfläche GNS-3

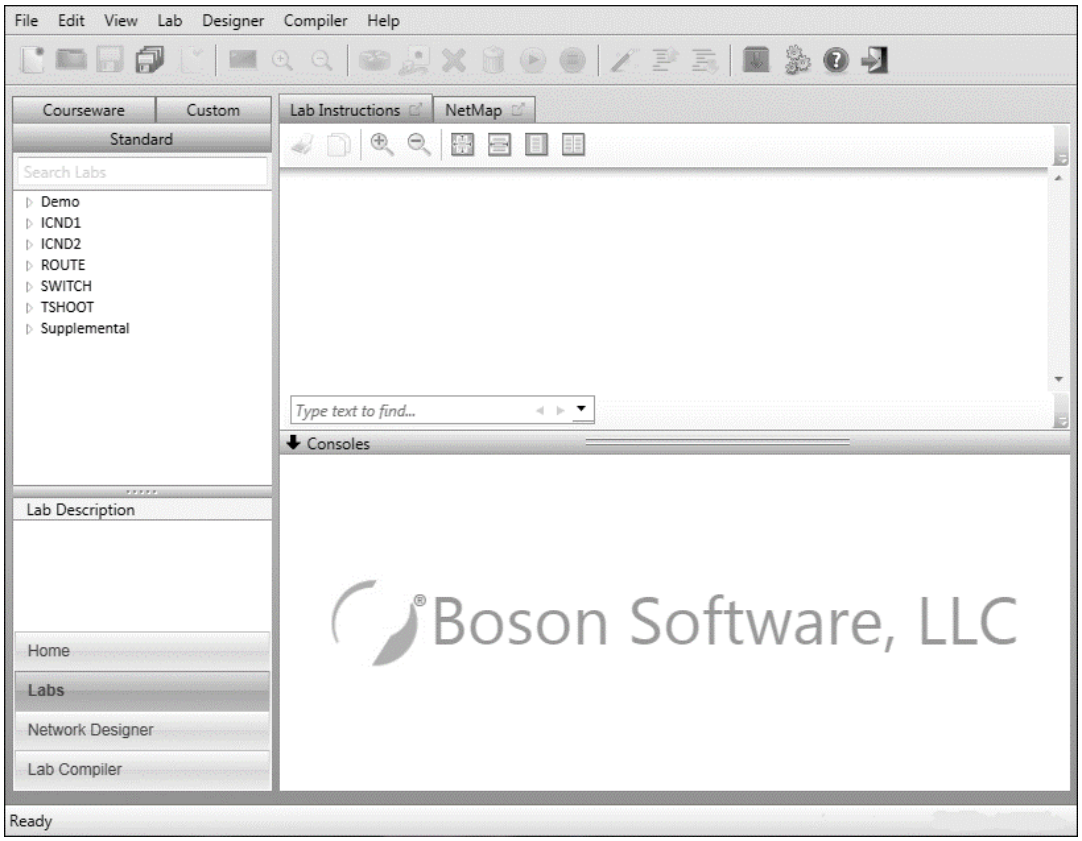

Abbildung 2.3, Oberfläche NetSim

Während bei Packet Tracer und GNS-3 eine Gerätepalette direkt zur Verfügung steht, muss sich der Anwender zuerst ausführlich mit der Boson Software NetSim beschäftigen, um ein einfaches Netzwerk aufzubauen. Dies ist für Anfänger nachteilig zu bewerten.

Weiterhin verfügen nur die Geräte unter Packet Tracer über eine grafische Desktop-Simulation und ein Konfigurationsmenü (Abbildung 2.4).

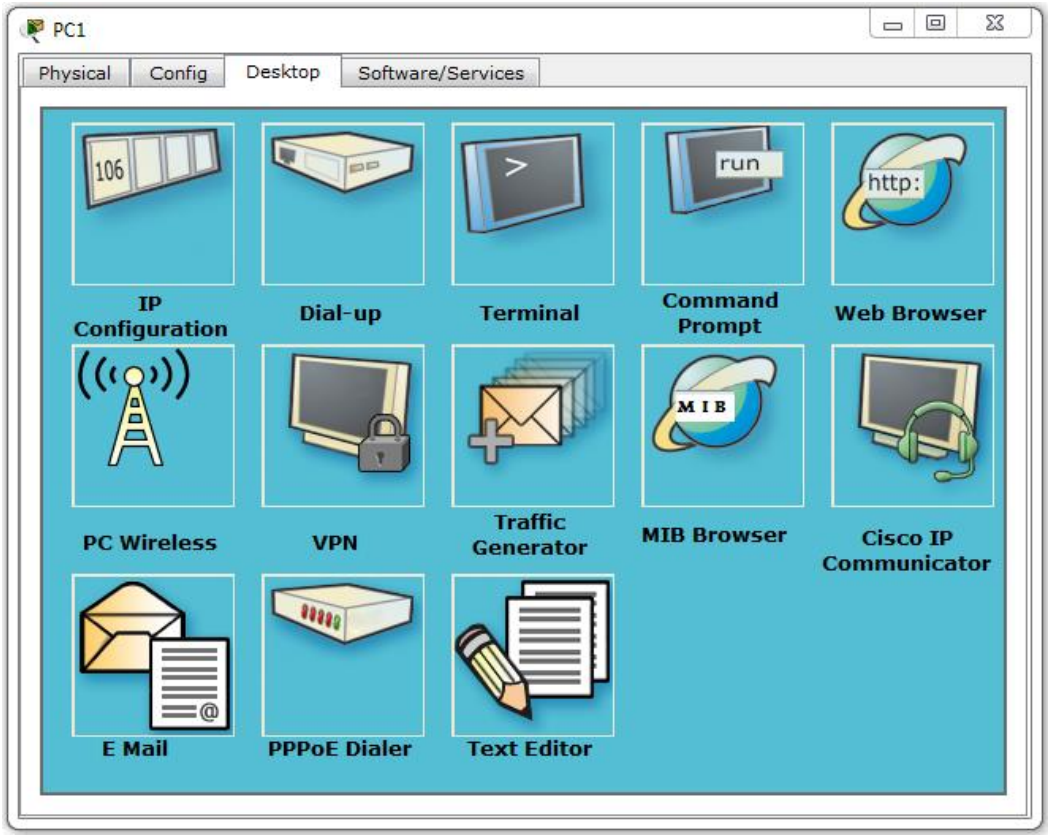

Abbildung 2.4, Desktopsimulation auf Packet Tracer-Geräten

Unter GNS-3 und NetSim sind die Geräte einzig über Eingabeaufforderungen zu steuern und zu konfigurieren. Dies bringt zunächst keine Nachteile mit sich, jedoch vermittelt der anschauliche Aufbau von Packet Tracer gerade Einsteigern ein besseres Verständnis bei der Konfiguration einzelner Geräte und hilft, die Verbindung zwischen Theorie und Praxis besser nachvollziehen zu können.

Der nächste Punkt behandelt die Verfügbarkeit dieser drei Programme und auf welchen Wegen diese zu erhalten sind. Cisco Packet Tracer ist für Mitglieder der

Cisco Networking Academy auf der zugehörigen Website[3] frei vorhanden. Bei der Installation des Programmes werden alle verfügbaren Geräte mitinstalliert, es sind also keine weiteren Schritte zur Arbeit mit diesem Programm notwendig. GNS-3 ist auf der entsprechenden Internetseite[4] ebenfalls kostenfrei zu erhalten und stellt eine Reihe wichtiger Geräte zur Verfügung, mit welchen die Netzwerksimulation durchgeführt werden kann. Einzig die Software NetSim ist kostenpflichtig ($99 - $349, je nach Einsatz, Stand Januar 2016) über die Boson Firmenwebsite[5] zu beziehen. Es besteht jedoch die Möglichkeit, die Software in einer eingeschränkten Demoversion zu testen.

Weiterhin wird der Funktionsumfang der vorgestellten Programme erörtert. Dieser gestaltet sich sehr unterschiedlich. Packet Tracer bietet eine große Auswahl an Geräten, welche in die Netzwerktopologien eingebracht werden können. Dabei kommen auch viele Multimediageräte (Tablets, Smartphones, TV-Geräte usw.) zum Einsatz. Diese dienen zwar nur zu Testzwecken, jedoch lassen sich so, besonders für Medienstudenten, praxisnahe Netzwerke realisieren. GNS-3 bietet im Direktvergleich mit Packet Tracer weniger Geräte zur Simulation. Ebenfalls beschränkt sich die Produktpalette auf essenzielle Netzwerkhardware (Switches, PCs, Hosts, Router usw.). Auch sind beispielsweise Router nicht von vornherein verfügbar. Diese müssen als Images nachträglich hinzugefügt werden. Die größte Auswahl an zu verwendender Hardware bietet das Programm NetSim (allein bis zu 42 Router). Die Geräte simulieren (ähnlich wie Packet Tracer) Geräte von Cisco Systems und arbeiten ebenfalls mit deren IOS Kommandozeile[6]. Weiterhin stellt die Software (je nach Version) bereits vorgefertigte Netzwerkszenarien, welche auf die verschiedenen Zertifikate der Cisco Networking Academy abgestimmt sind.

Abschließend wird auf die unterschiedlichen Funktionsweisen der einzelnen Programme eingegangen und die damit verbundenen Vor- und Nachteile

[3] [Web02]

[4] [Web03]

[5] [Web04]

[6] Cisco-eigene Kommandozeilensoftware

aufgezeigt. Packet Tracer simuliert alle enthaltenen Geräte innerhalb des Programms, d.h. es werden keine weiteren Ressourcen am Anwenderrechner benötigt, als jene, welche das Programm selbst nutzt. Dies ist bezüglich der Computerausstattung von Vorteil, da eine moderate Hardwareausstattung genügt, um Packet Tracer betreiben zu können. Jedoch stehen dadurch die simulierten Geräte nur mit eingeschränkten Funktionen zur Verfügung (z.B. einfachere IOS-Versionen auf Routern und Switches). GNS-3 dagegen emuliert sämtliche, zur Verfügung stehende Hardware über integrierte Emulationssoftware (u.a. VirtualBox). Dadurch wird es dem Anwender ermöglicht, realitätsgetreu mit den zur Verfügung gestellten Geräten zu arbeiten, d.h. GNS-3 emuliert die Gerätesoftware 1:1. Weiterhin positiv ist die Einbindung der Software Wireshark in das Programm, welche auf das erstellte Netzwerk anwendbar ist. Nachteilig zu erwähnen, ist der damit verbundene Ressourcenverbrauch, welcher proportional zur Anzahl der verwendeten Geräte ansteigt und auch modernere Rechner stark belasten kann[7]. Des Weiteren sind die Möglichkeiten des Switchings unter GNS-3 stark eingeschränkt, was ebenfalls als Nachteil zu behandeln ist. Die Software NetSim verknüpft diese beiden Methoden. Die vorhandenen Geräte (ähnlich wie bei Packet Tracer) werden simuliert. Jedoch verfügt das Programm über einen Emulationsserver, welche es dem Benutzer ermöglicht, das erstellte Netzwerk zu emulieren und reale Hardware daran anzubinden. Dazu wird allerdings eine weitere Clientsoftware benötigt. Positiv zu bewerten, ist die Möglichkeit, reale Hardware in die Tests mit einzubeziehen, um so die Simulation so praxisnah wie möglich zu gestalten. Allerdings wird dazu zum einen die zusätzliche Clientsoftware benötigt, zum anderen auch mehrere Geräte, was gerade für Privatanwender als unvorteilhaft anzusehen ist.

Wie erläutert, zeigen alle 3 Softwarelösungen Stärken und Schwächen. Weiterhin spielt letztlich das Einsatzziel eine entscheidende Rolle bei der Programmauswahl. Zusammenfassend, unter Betrachtung der Vor- und Nachteile, zeigt sich jedoch, dass Packet Tracer für eine Einführung in die Thematik der Netzwerktechnik durch den grafischen Aufbau, die zur Verfügung stehenden Geräten und die simulierte

[7] [Web07]

CLI-Oberfläche am besten geeignet ist. Die Cisco Networking Academy setzt Packet Tracer ebenfalls in den firmeneigenen Kursen für das Erlangen des CCNA-Zertifikats, welches ebenfalls Grund- und weiterführende Kenntnisse der Netzwerktechnik vermittelt, ein. Dies trifft auch auf das im Rahmen dieser Arbeit entstandene Praktikum zu.

3 Cisco Packet Tracer

3.1 Einführung und Überblick

3.1.1 Was ist Packet Tracer?

Bei der Software Packet Tracer handelt es sich um ein Netzwerksimulationsprogramm der Firma Cisco Systems. Hauptsächlich wird es von Studenten der Cisco Network Academy genutzt. Es wird zur Simulation von verschiedenen Netzwerken verwendet und hilft, grundlegende und weiterführende Kenntnisse in der Netzwerktechnik zu erlangen. Des Weiteren können verschiedene Paket- und Fehleranalysen durchgeführt werden, um die Kommunikation und Konnektivität einzelner Geräte eines Netzwerkes untereinander zu verstehen. Es stehen verschiedene Netzwerkkomponenten zur Verfügung, um unterschiedliche Szenarien darzustellen (Heimnetzwerk, Firmennetzwerk, geografisch begrenzte Netzwerke usw.), um die Unterschiede und Funktionsweisen diverser Netzwerkgeräte, in Abhängigkeit von deren Verwendungszweck, aufzuzeigen. Durch zahlreiche Visualisierungsmöglichkeiten (Protokollverfolgung, Kollisionsanzeige usw.) bietet Packet Tracer die Möglichkeit, besonders Anfängern die verschiedenen Arbeitsweisen der Geräte innerhalb eines Netzwerkes verständlich zu vermitteln. Durch die Möglichkeit, sich bei Bedarf jeden einzelnen Schritt nach dem OSI – Referenzmodell kategorisiert anzeigen zu lassen, trägt Packet Tracer ebenfalls zu einem besseren Verständnis dieses, für die Netzwerktechnik extrem wichtigen Modells bei.

3.1.2 Oberfläche und Elemente

Im Folgenden wird Packet Tracer (Version 6.0.1) näher betrachtet und sämtliche wesentliche Bedienelemente aufgezeigt. Dazu erfolgt eine kurze Zusammenfassung über die Verwendung des jeweils betrachteten Elements. Nach

dem Start des Programmes erscheint die Hauptoberfläche der Software (Abbildung 3.1).

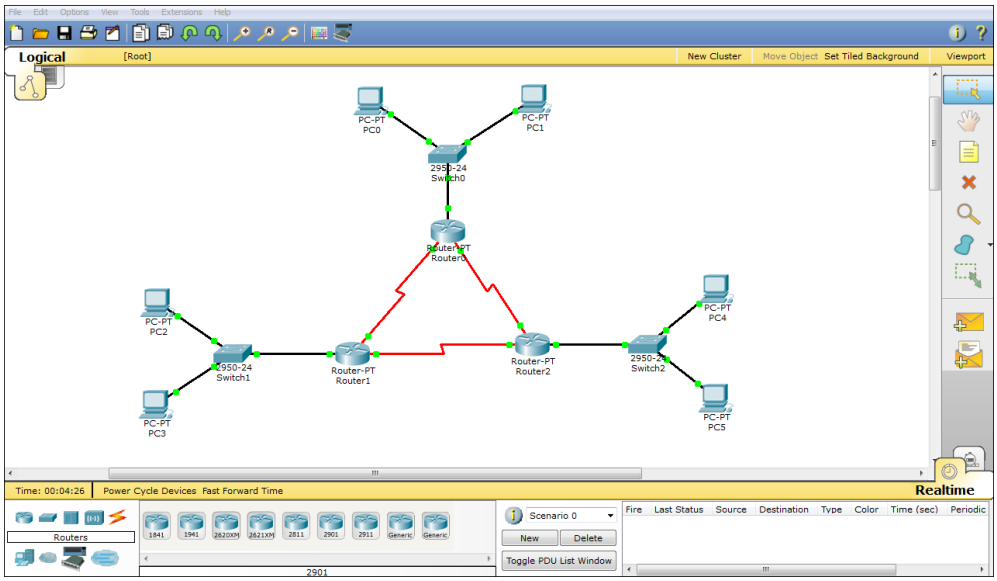

Abbildung 3.1, Hauptfenster Packet Tracer

Auf dieser finden sämtliche Interaktionen mit dem Programm statt. Sie besteht aus verschiedenen Bestandteilen:

Die Menüleiste (Abbildung 3.2).

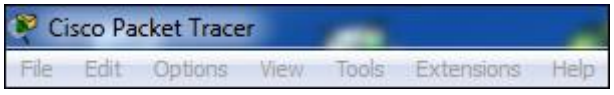

Abbildung 3.2, Menüleiste Packet Tracer

Die obere Toolbar (Abbildung 3.3).

Abbildung 3.3, Obere Toolbar Packet Tracer

Die obere Werkzeugliste stellt verschiedene Verknüpfungen zu den gebräuchlichsten Funktionen (Neu, Öffnen, Speichern usw.) aus der Menüleiste bereit, um auf diese schneller zugreifen zu können.

Die Arbeitsfläche (Abbildung 3.4).

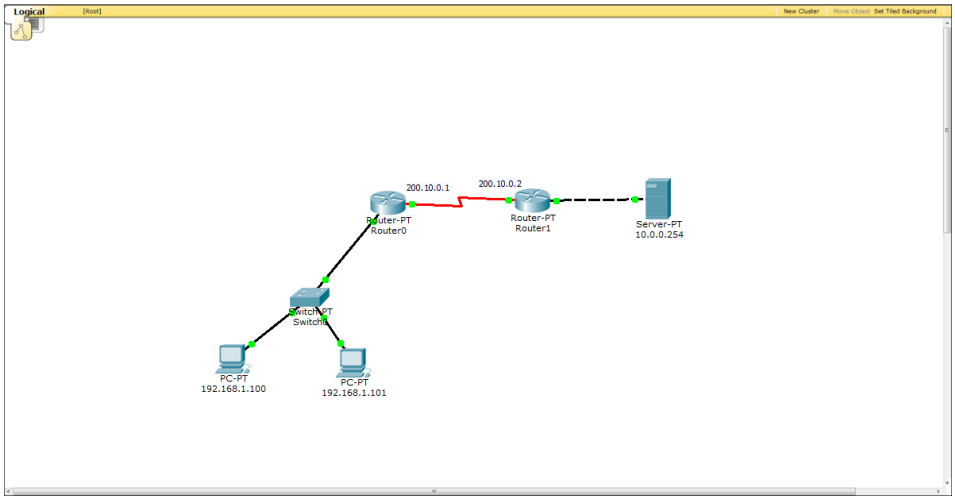

Abbildung 3.4, Arbeitsfläche Packet Tracer

Auf der Hauptarbeitsfläche werden sämtliche Netzwerkkomponenten, die für die Simulation eines Netzwerks benötigt werden, platziert, verwaltet und konfiguriert. Dies geschieht durch logische Verknüpfungen dieser untereinander, jedoch unter keinem realen Maßstab.

Die rechte Toolbar (Abbildung 3.5).

Abbildung 3.5, Rechte Toolbar Packet Tracer

Die rechte Toolbar stellt Werkzeuge bereit, um mit den auf der Arbeitsfläche platzierten Komponenten zu interagieren. Neben einem Auswahl- und Löschwerkzeug findet sich ebenfalls ein Text- und Zeichenwerkzeug, um beispielsweise durch Beschriftung und optische Abgrenzung eine bessere Übersichtlichkeit des gesamten Netzwerkes zu erreichen.

Die untere Toolbar (Abbildung 3.6).

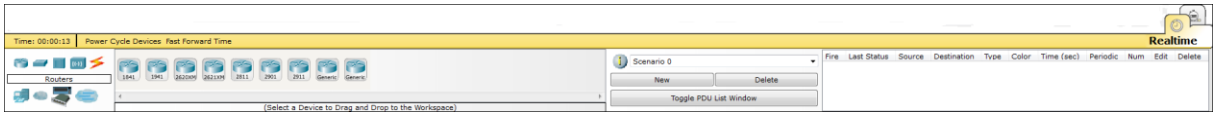

Abbildung 3.6, Untere Toolbar Packet Tracer

Die untere Toolbar listet sämtliche, zur Verfügung stehenden Geräte auf. Außerdem sind hier alle aktuellen Szenarien, sowie Paketübertragungen aufgeführt.

3.1.3 Unterstützte Hardware

Packet Tracer offeriert eine Vielzahl von Geräten, welche in den Simulationen verwendet werden können. An dieser Stelle erfolgt eine Aufschlüsselung der für das Praktikum wichtigsten integrierten Hardware, welche tabellarisch aufgeführt ist. Einige der Geräte weisen dabei freie Fächer auf: Interfacekartenslots und Modulkartenslots. Interfacekarten fügen weitere Interfaces hinzu (z.B. Ethernet-Ports), Modulkartenslots fügen weiter Steckplätze für Interfacekarten hinzu. Die Verfügbarkeit solcher Slots ist in der Beschreibung mit angegeben. Eine vollständige Geräteliste findet sich als Anlage (vgl. Anlagen, Teil 2, Geräteliste).

3.1.3.1 Router

1841	
Cisco-Router mit zwei integrierten FastEthernet-Ports, einem USB-Anschluss und zwei Slots zur Erweiterung mit Interfacekarten. Im Praktikum am häufigsten, zum Einsatz kommender Router.	

Tabelle 3.1, Häufig verwendete Geräte (Router)

3.1.3.2 Switches

2950 – 24    Cisco-Switch mit 24 integrierten FastEthernet-Ports. Im Praktikum am häufigsten, zum Einsatz kommender Switch.

Tabelle 3.2, Häufig verwendete Geräte (Switches)

3.1.3.3 Endgeräte

PC    Handelsüblicher PC, mit verschiedenen Interfaces ausstattbar und integrierter Desktopoberfläche. Essenziell für sämtliche Aufgaben des Praktikums.
Laptop    Handelsüblicher Laptop, mit verschiedenen Interfaces ausstattbar und integrierter Desktopoberfläche. An Stelle eines PCs verwendbar.
Server    Handelsüblicher Server mit einem integriertem FastEthernet-Port, sowie einen Slot zur Erweiterung mit Interfacekarten. Grafische Benutzeroberfläche. Für viele Einzelaufgaben des Praktikums notwendig.

Tabelle 3.3, Häufig verwendete Geräte (Endgeräte)

3.1.3.4 Sonstige

Hub    Cisco-Hub mit 6 integrierten FastEthernet-Ports, sowie 4 Slots zur Erweiterung mit Interfacekarten.
Generic Cloud    Repräsentiert eine Cloud zu Simulationszwecken. 10 Slots zur Erweiterung mit Interfacekarten. Essenziell für das Komplexbeispiel.
DSL Modem    DSL Modem mit integriertem FastEthernet-Port und Telefonkabelanschluss. FastEthernet-Interface ist durch andere Inferfaces ersetzbar. Essenziell für das Komplexbeispiel.

Tabelle 3.4, Häufig verwendete Geräte (Sontige)

3.1.3.5 Module

Viele der bereits erwähnten Geräte unter Packet Tracer können um zusätzliche Funktionen erweitert werden. Dazu stellt das Programm pro Gerätegruppe mehrere Module zur Verfügung, welche nachträglich installiert werden können, um den Funktionsumfang ausgewählter Hardware zu erweitern. Eine komplette Liste dieser Module findet sich im Anhang (vgl. Anlagen, Teil 3, Modulliste).

3.2 Echtzeit- und Simulationsmodus

Das Kernfeature von Packet Tracer liegt in den beiden zur Verfügung stehenden Modi: dem Echtzeitmodus und dem Simulationsmodus. Der Echtzeitmodus simuliert das eingerichtete Netzwerk unter realen Zeitumständen. Wird beispielsweise mit Ping die Erreichbarkeit eines Netzwerkteilnehmers getestet, findet dieser Schritt im Echtzeitmodus wie in einer realen Umgebung statt. Es werden Netzwerke eingerichtet und konfiguriert. Für die eigentliche Simulation und Analyse der verwendeten Topologie spielt der Simulationsmodus die größere Rolle. In dieser Betriebsart werden sämtliche Datenübertragungen (ICMP-Pakete bei Ping, SMTP-Pakete beim Empfangen einer Email über den integrierten Email-Client etc.) visualisiert dargestellt. Diese Übermittlungen werden mit einem Briefsymbol symbolisiert. Deren Transportweg kann somit schrittweise verfolgt werden (Abbildung 3.7).

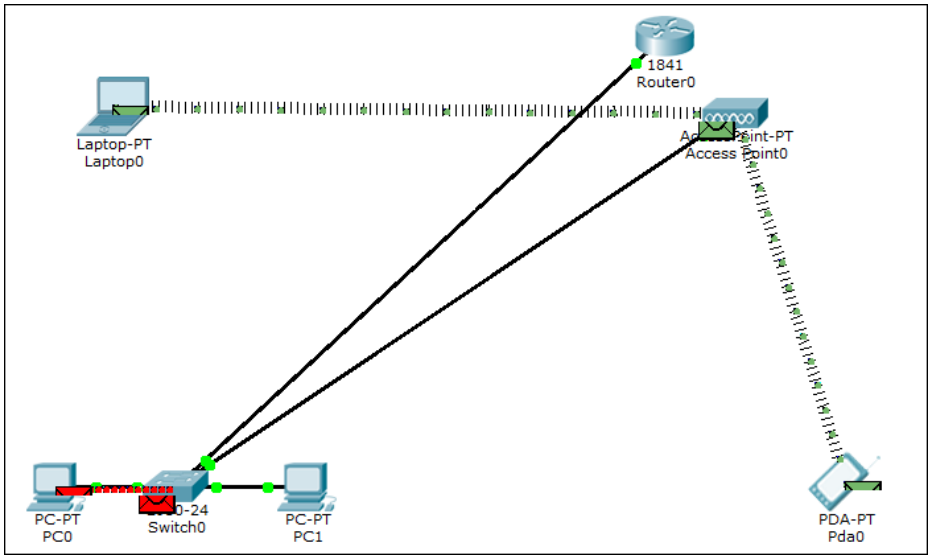

Abbildung 3.7, Paketübertragung im Simulationsmodus

Weiterhin ist es möglich, eine detailgenaue Ansicht der Paketdaten, basierend auf dem OSI-Modell zu betrachten (Abbildung 3.8).

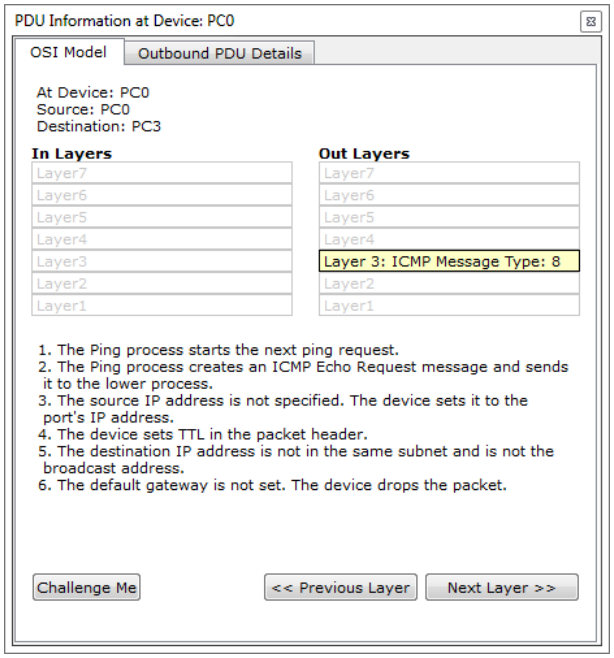

Abbildung 3.8, Detailansicht eines Datenpakets unter Packet Tracer

Dies macht es möglich, einen genauen Einblick in die Funktionsweisen verschiedener Protokolle zu erlangen und eignet sich somit besonders, die Grundlagen der Netzwerktechnik zu verstehen und besitzt damit die Eigenschaft, theoretische Prinzipien praxisnah zu vermitteln.

3.3 CLI – Command Line Interface

Das CLI ist unter Packet Tracer auf Switches und Routern verfügbar. Es dient der Konfiguration dieser Geräte. Diese Art der Geräteprogrammierung ist anspruchsvoller, als die manuelle Einrichtung per grafischer Oberfläche, jedoch auch praxisnäher, da dies die häufigste Administrationsart darstellt. Per Tabulator Taste lassen sich eingegebene Befehle vervollständigen, per Enter Taste bestätigen. Lässt man einem Befehl ein Leerzeichen und ein Fragezeichen folgen und schickt diesen Befehl ab, listet die Konsole sämtliche Folgevarianten auf das eingegebene Kommando auf. Unter Packet Tracer steht das CLI nicht in gesamtem Umfang zur Verfügung. Dennoch werden zahlreiche Befehle zur Konfiguration der Geräte unterstützt, von welchen die wichtigsten, im Praktikum zur Anwendung kommenden, nachfolgend aufgeführt sind.

Befehl	**Wirkung**
enable	Bereitet das Gerät auf Konfiguration vor.
configure terminal	Aktiviert den globalen Konfigurationsmodus.
ip address xxx	Weist einem Interface die IP-Adresse xxx zu.
ip dhcp pool [Name]	Fügt der Konfiguration ein DHCP-Pool hinzu und öffnet dessen Konfiguration.
network xxx	Fügt der Konfiguration das Netz xxx hinzu.
ip dhcp excluded-address	Schließt eine IP-Adresse vom DHCP-Pool aus.
default-router	Setzt das Default Gateway eines DHCP-Pools.
copy run start	Speichert die aktuelle Konfiguration.
router rip	Öffnet die Konfiguration von RIP Routing.
show	Zeigt bestimmte Informationen an.

exit	Verlässt die aktuelle Konfiguration.
end	Verlässt den globalen Konfigurationsmodus.

Tabelle 3.5, Versuchsrelevante CLI-Befehle

Eine vollständige Dokumentation zu den Befehlen lässt sich im IOS-Handbuch auf der Homepage[8] von Cisco Systems einsehen.

[8] [Web05]

4 Praktikum

4.1 Einführung

Das im Rahmen dieser Diplomarbeit entwickelte Praktikum umfasst 4 aufeinander aufbauende Versuche zum Thema Netzwerktechnik. Diese werden von Studenten der Kommunikationstechnik/Netzwerktechnik durchgeführt, um deren Kenntnisse in diesem Bereich zu erweitern und zu festigen. Dabei werden die Funktionsweisen existierender Technologien abgehandelt und den Praktikanten in Verbindung mit simulierten Beispielen vermittelt. Theoretisch orientiert sich das Praktikum an der parallel laufenden Vorlesung zu dem Thema Netzwerktechnik und Administration.

4.2 Aufbau

Die Versuche sind chronologisch aufgebaut und basieren aufeinander, d.h. Versuch 2 setzt die gewonnenen Kenntnisse aus Versuch 1 voraus und so weiter. Des Weiteren bestehen die einzelnen Praktika aus mehreren Teilaufgaben, welche den Anwender schrittweise durch die Versuche führt. Dabei werden Erklärungen zu Technologien, Diensten und deren Einrichtung jeweils nur einmal ausgeführt, um einen Lernprozess bei den teilnehmenden Studenten zu veranlassen. Zu Beginn jeder Teilaufgabe sind die zu verwendenden Hardwarekomponenten tabellarisch aufgelistet. Zur Aufbereitung der erworbenen Kenntnisse finden sich am Ende jedes Versuches fachliche Fragen, welche sich inhaltlich auf die behandelten Themen im Versuch beziehen. Ebenfalls sind Randinformationen in den Fließtext der Praktikumsanleitungen eingebracht, welche fachlich relevante Hinweise zu den aktuell behandelten Problematiken liefern.

4.3 Versuchsumgebung

Die Durchführung des Praktikums erfordert keine speziellen technischen Voraussetzungen. Lediglich ein handelsüblicher PC wird für die Installation und den Betrieb der Software Packet Tracer benötigt. Die minimalen Systemvoraussetzungen[9] für ein einwandfreies Funktionieren des Programmes (Version 6.0.1) sind mit einer Prozessorleistung von 2,53GHz (Intel Pentium 4 o.ä.) und einer Arbeitsspeichergröße von 512MB moderat und sollten von jedem aktuellen System erreicht werden.

4.4 Verwendete Technologien

Nachfolgendend werden die wichtigsten Technologien, welche im Praktikum Anwendung finden, alphabetisch geordnet aufgelistet und kurz erläutert. Dies dient als Einblick und führt den Leser an diese heran. Um weiterführende Informationen zu den einzelnen Diensten, Protokollen und Prinzipien einzuholen, sind anderweitige Literaturquellen heranzuziehen (vgl. Literaturverzeichnis).

ARP: Ein Protokoll zur Ermittlung der MAC-Adresse anhand der IP-Adresse.

CSMA / CD: Mechanismus zur Kollisionsverhinderung.

DHCP: Protokoll zur Verwaltung und Verteilung von IP-Konfigurationen.

DNS: Verfahren zur Auflösung von IP-Adressen in Namen und andersherum.

Firewall: Mechanismus zur Kontrolle von ein- und ausgehenden Daten.

ICMP: Protokoll zur Übertragung von Informationen und Fehlermeldungen.

IMAP: Kommunikationsprotokoll zur Verwaltung von Emails auf einem geografisch entfernten Server.

LAN: Bezeichnung für ein lokales Netzwerk.

---

[9] Vgl. Packet Tracer User Manual, in der Software enthalten

MAN: Bezeichnung für ein Netzwerk innerhalb großer Städte oder Regionen.

NAT: Verfahren zur Übersetzung von IP-Adressen.

NAPT: Verfahren zur Übersetzung von IP-Adressen und Portnummern.

Ping: Netzwerktool, um die Erreichbarkeit anderer Netzteilnehmer zu testen**.**

POP3: Kommunikationsprotokoll zur Abholung von Emails.

RIP: Protokoll zur automatischen Erstellung von Routingtabellen.

Routing: Verfahren zur Wegebestimmung eines Datenstroms.

SMTP: Kommunikationsprotokoll zur Übertragung von Emails.

VLAN: Virtuelle Teilnetze innerhalb eines physikalischen Netzes.

WAN: Bezeichnung für ein Netzwerk, welches große geografische Bereiche abdeckt.

WLAN: Bezeichnung für kabellose Netzwerke.

4.5 Praktikumsbetrachtung

Im Folgenden werden die entwickelten Versuche einzeln aufgeschlüsselt. Dabei wird insbesondere auf die Ziele eingegangen, welche mit dem Absolvieren des jeweiligen Praktikums erreicht werden. Außerdem werden Fragestellungen der Versuche aufgearbeitet und Lösungsmuster vorgestellt. Auf genaue Gerätebezeichnungen wird in dieser Aufteilung verzichtet, da die didaktische und methodische Vorgehensweise bei der Erarbeitung des Praktikums im Vordergrund steht. Die detaillierten Bezeichnungen sind den Versuchsanleitungen im Anhang zu entnehmen.

4.5.1 Versuch 1

Versuch 1 wird als Einführung in die Thematik behandelt, gibt einen Überblick über die Grundfunktionen der Software Packet Tracer und beschäftigt sich mit

einfachsten Technologien, die in der Netzwerktechnik Anwendung finden. Des Weiteren wird in das, in der Netzwerktechnik extrem wichtige, OSI – Modell eingeführt. Die Bearbeitungszeit dieses ersten Versuchs beläuft sich auf 60 Minuten.

Die erste Teilaufgabe des Versuches behandelt eine einfache Direktverbindung zweier handelsüblicher Computer. Dabei werden die Studenten vorerst angewiesen, ein Standard Netzwerkkabel zur Vernetzung der Geräte zu verwenden. Die Software signalisiert an dieser Stelle, dass keine Übertragung stattfinden kann, da es sich bei dem verwendeten Kabel nicht um das spezielle Crossoverkabel mit gekreuzten Adern handelt (Abbildung 4.1).

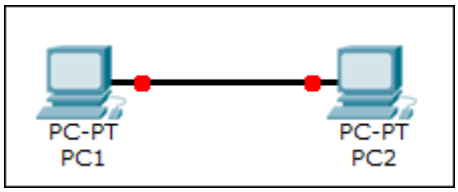

Abbildung 4.1, Verbindung zweier Computer mittels Standardkabel

Rot gekennzeichnete Verbindungen teilen dem Anwender mit, dass eine Kommunikation nicht möglich ist. Mit diesem Beispiel wird aufgezeigt, dass eine Verbindung nur stattfinden kann, wenn die Signaladern im Kabel selbst gekreuzt sind. Das Ersetzen des Standardkabels mit dem vorher erwähnten Crossoverkabel ermöglicht umgehend eine Kommunikation zwischen den beiden Rechnern. Packet Tracer stellt dies sofort mit Hilfe einer grünen Kennzeichnung dar (Abbildung 4.2).

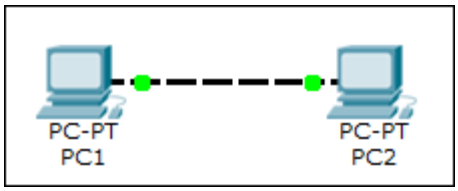

Abbildung 4.2, Verbindung zweier Computer mittels Crossoverkabel

Im zweiten Teilabschnitt des Versuches wird weiterführend eine auf dem ICMP-Protokoll basierende Paketübertragung sowohl im Echtzeitmodus, als auch im Simulationsmodus veranlasst, um das fehlerfreie Funktionieren der erfolgten

Verbindung zu demonstrieren. Im Simulationsmodus verfolgen die Studenten die Paketübertragung visualisiert, um diese nachvollziehen zu können.

Teilaufgabe 3 lässt die Studenten das auf dem ICMP-Protokoll basierende Tool Ping ausführen. Dazu wird die Kommandozeile verwendet, welche auf den unter Packet Tracer verfügbaren PCs zur Verfügung steht (Abbildung 4.3).

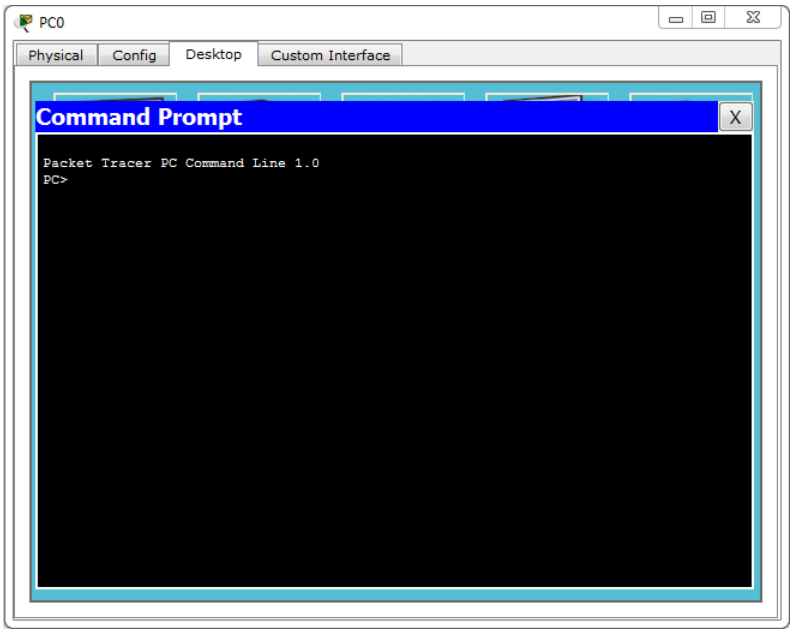

Abbildung 4.3, PC-Kommandozeile unter Packet Tracer

Dies erläutert den Umgang mit diesem wesentlichen Diagnosewerkzeug und verdeutlicht dessen Funktion. Ebenso wird den Studenten nahegebracht, dass dieses Werkzeug in der Netzwerktechnik eingesetzt wird, um festzustellen, ob ein bestimmtes Gerät innerhalb eines Netzwerkes logisch erreichbar ist.

Nach Abschluss dieser einführenden Abschnitte thematisiert Teilaufgabe 4 die Verknüpfung mehrerer Netzwerkgeräte. Zu Beginn verbinden die Studierenden 4 handelsübliche Computer über einen Hub. Die zu verwendenden Kabeltypen werden nun nicht mehr angegeben und müssen vom Anwender selbst gewählt werden. Ist diese Konstellation aufgebaut worden, wird eine Dateiübertragung zwischen zwei, sich im Netz befindlichen PCs gestartet und im Simulationsmodus verfolgt (Abbildung 4.4).

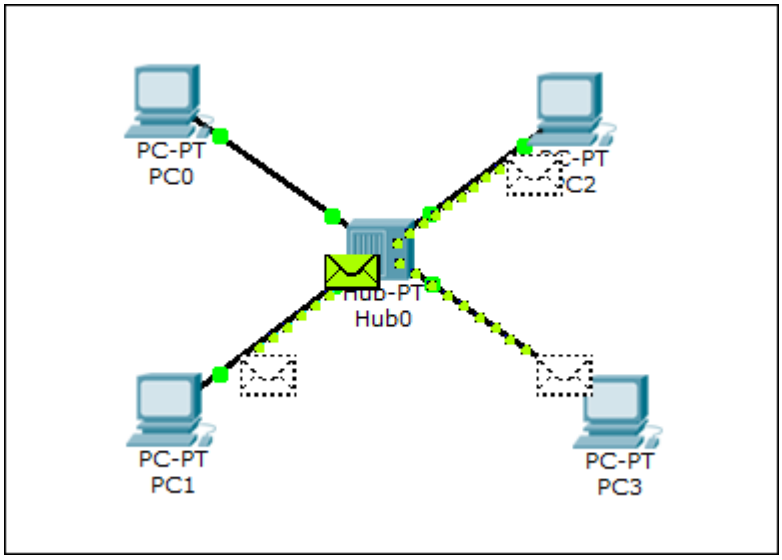

Abbildung 4.4, Simulierte Dateiübertragung mittels Hub

Durch die Beschaffenheit des Hubs und dessen Funktionsbeschränkung auf Schicht 1 des OSI-Modells findet eine Übertragung an alle, sich im Netz befindlichen Komponenten statt, welches die Software dementsprechend darstellt. Eine gezielte Übertragung an einen bestimmten Netzteilnehmer ist nicht möglich. Durch die dargestellte Simulation wird dem Anwender die Funktionsweise von Hubs verdeutlicht und vermittelt damit Kenntnisse über Verhaltensweisen dieser Geräte. Weiterhin beinhaltet der Versuch Einsatzgründe für Hubs und erklärt warum diese heutzutage stetig weniger Anwendung finden. Im nächsten Schritt wird der Student aufgefordert, den Hub durch einen Switch zu tauschen, um auf eine aktuellere Technologie überzuleiten und Gründe aufzuzeigen, warum Switches den Hub vom Markt verdrängt haben. Durch eine erneut veranlasste Paketübertragung und deren Betrachtung im Simulationsmodus wird ersichtlich, dass Switches dazu in der Lage sind, Empfänger der zu übermittelnden Daten anhand von Informationen aus Schicht 2 des OSI-Modells im Netz zu identifizieren und dadurch gezielte Adressierungen im Netz ermöglicht werden (Abbildung 4.5)

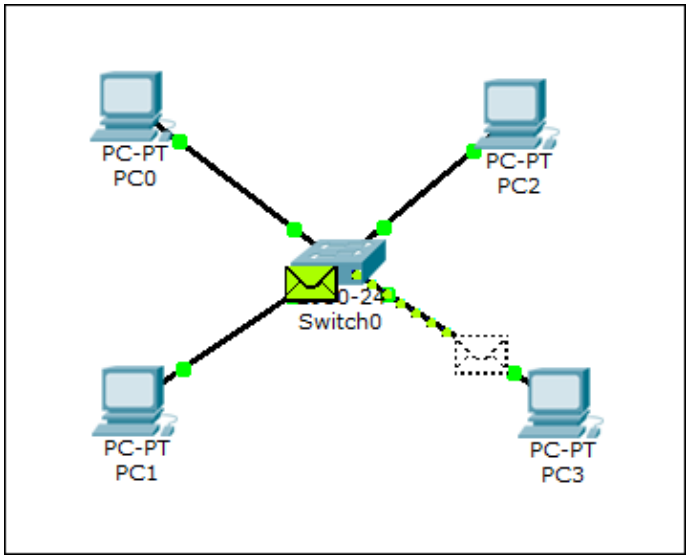

Abbildung 4.5, Simulierte Dateiübertragung mittels Switch

Lösungsansätze zu Versuch 1

Unter Teilaufgabe 4 werden die Studenten angewiesen, allen 4 PCs eine statische IP zuzuweisen. Diese sollen sich im selben Netz befinden. Da es sich um ein Klasse C Netz handelt, kann hier beispielsweise das Netz der Form 192.168.0.0 /24 verwendet werden (/24 steht für einen 24-Bit-Netzanteil, also die Subnetzmaske 255.255.255.0). Als Kabel kommt ein Standard RJ-45 Kupferkabel ohne gekreuzte Adern zum Einsatz.

Lösungen zu den Aufgaben am Ende des Versuches:

1. Welche Kabelart ist für eine Direktverbindung zweier PCs geeignet und was macht diese besonders?

Für eine Direktverbindung zwischen zwei PCs wird in der Praxis ein Crossoverkabel verwendet. Die Besonderheit bei dieser Kabelart liegt in der Kreuzung bestimmter Kabeladern (1-2, sowie 3-6) in einem der beiden Anschlüsse, um Sende- und Empfangsvorgänge realisieren zu können.

2. Nennen Sie die Unterschiede zwischen Hubs und Switches. Beziehen Sie sich dabei auch auf das OSI-Referenzmodell.

Im Gegensatz zu Hubs sind Switches in der Lage, den Empfänger eines Datenpakets auszumachen und dieses gezielt an diesen zu vermitteln. Dies resultiert daraus, dass Hubs nur auf Schicht 1, der Bitübertragungsschicht, arbeiten. Switches sind ebenfalls dazu fähig, gleichzeitig zu senden und zu empfangen. Dies spiegelt sich auch in der Arbeitsgeschwindigkeit dieser wider, welche dadurch höher ist, als die eines Hubs.

3. Was bedeutet ICMP?

ICMP (Internet Control Message Protocol) ist ein Protokoll, welches dem Informationsaustausch innerhalb IPv4-basierter Netzwerke dient. Das Tool Ping verwendet ICMP als Übertragungsprotokoll.

4. Ermitteln Sie 4 IP Adressen, welche sich einem Klasse C Netzwerk zuordnen lassen.

192.168.0.1 – 192.168.0.2 – 192.168.0.3 – 192.168.0.2

4.5.2 Versuch 2

Der zweite Versuch führt weiter in die Netzwerktechnik ein und vermittelt dem Anwender grundlegendes Wissen über weitere Dienste und Technologien der Netzwerktechnik. Dabei baut er auf den bereits erworbenen Kenntnissen von Versuch 1 auf. Die Bearbeitungszeit beträgt 90 Minuten. Erneut ist der Gesamtversuch in einzelne Teilaufgaben unterteilt, welche sich mit jeweils einer Teilthematik befassen.

Teilaufgabe 1 behandelt die Einrichtung und die grundlegende Funktionsweise eines DHCP-Servers und dem dazugehörigen gleichnamigen Dienst. In diesem Szenario werden die Studenten angewiesen, 3 PCs über einen Switch in einem Netzwerk zusammenzufassen. Außerdem wird ein Server an dieses Netz angebunden, welcher hier softwareseitig erstmalig zum Einsatz kommt. Der Anwender wird zunächst aufgefordert, in den IP-Einstellungen der PCs die Zuweisungsmethode auf DHCP umzustellen. Dieser bleibt erwartungsgemäß erfolglos, da noch keine Konfiguration auf Seiten des DHCP-Servers vorgenommen wurde (Abbildung 4.6).

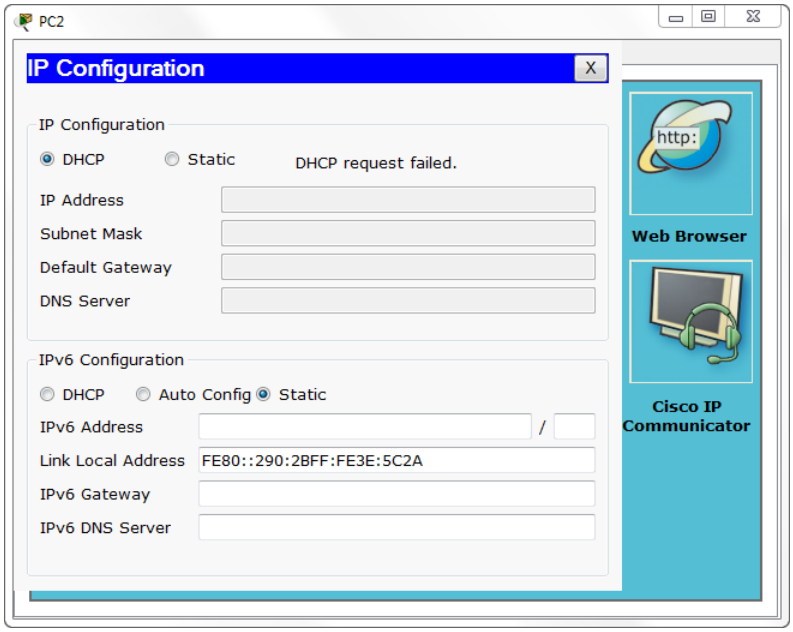

Abbildung 4.6, Erfolglose DHCP-Anfrage

Diese Erkenntnis stellt sich ebenfalls bei den Studenten ein, welche sich in einem nächsten Schritt mit der Konfiguration des DHCP-Servers beschäftigen. Der hinzugefügte Server verfügt bereits über eine DHCP-Konfigurationsoberfläche, in welche der Anwender jetzt noch die gewünschten Parameter eintragen muss (Start – End IP Adresse, Default Gateway, DNS Server). Dies beschreibt dem Benutzer, dass ein Administrator in einem DHCP-Server grundlegend eine Netzwerkkonfiguration, bestehend aus einem Pool an IP-Adressen, sowie zum Netz gehörigen Gateways und einem eventuell vorhandenen DNS-Server, bereitstellt. Diese weist der Server dann einem Client auf Anfrage automatisiert zu. Damit diese erfolgreich realisiert werden kann, benötigt der Server ebenfalls noch eine IP-Adresse. Da in diesem Beispiel der Server lediglich über einen Switch in das Netz eingebunden ist, muss dessen IP-Adresse im gleichen Netz wie der zu verteilende IP-Bereich liegen, da sonst keine Kommunikation mit den restlichen Netzkomponenten möglich ist. Diese müssen die Studenten hier selbstständig festlegen, wodurch der Umgang mit IPv4-Adressen und deren Verwendung geschult wird. Nach erfolgreicher Einrichtung der DHCP-Technologie wird anhand einer DHCP-Anfrage eines Clients simuliert, wie eine solche Abfrage umgesetzt wird. Dabei wird im Simulationsmodus der Software die Zuweisungsmethode eines PCs im Netz von Statisch auf DHCP umgestellt. Folglich kann der Anwender

sämtliche Paketübertragungen zwischen Client und DHCP-Server verfolgen, welche letztlich zu einer erfolgreichen Übermittlung der angeforderten Netzwerkkonfiguration führt (DHCPDISCOVER, DHCPOFFER, DHCPREQUEST). Die Detailansicht der Pakete gibt zusätzlich Aufschluss über die einzelnen Schritte, bezogen auf die verschiedenen Schichten des OSI-Modells (Bsp. Abbildung 4.7).

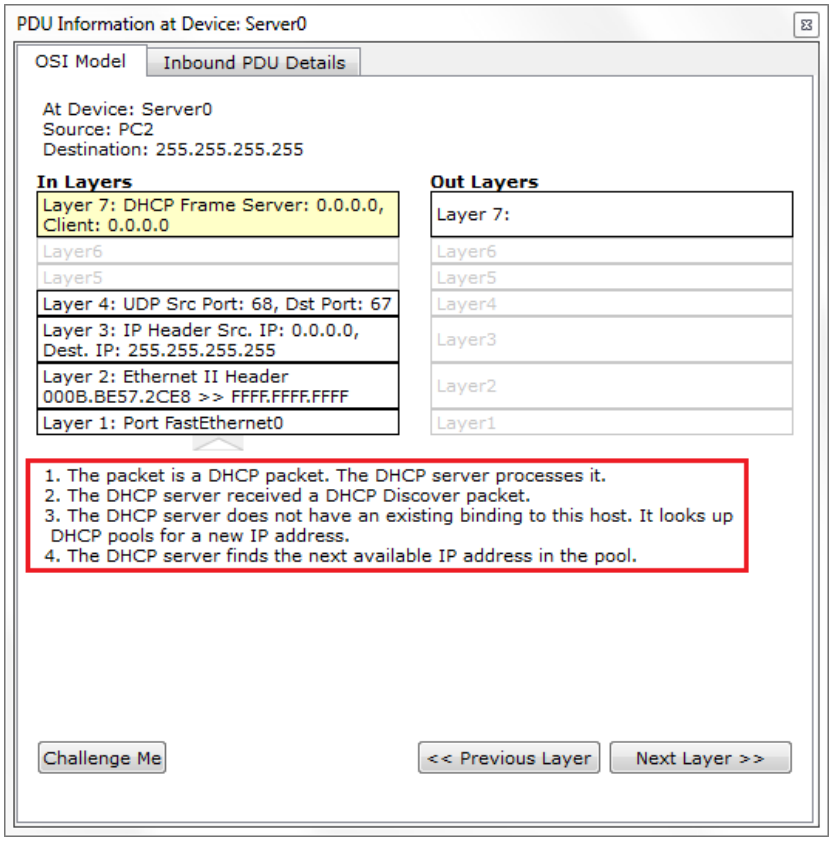

Abbildung 4.7, OSI-Detailansicht einer DHCPDISCOVER-Paketübertragung

Teilaufgabe 2 behandelt hauptsächlich den Dienst DNS. Den Studierenden wird dabei einer der wichtigsten existierenden Dienste nähergebracht. Um die Funktionsweise dieses Dienstes detaillierter zu betrachten, wird erneut ein Server herangezogen, welcher als DNS-Server arbeitet und von den bearbeitenden Studenten eingerichtet und getestet wird. Zusätzlich zur Einrichtungsanleitung werden relevante Randinformationen zu DNS zur Verfügung gestellt, etwa den Gründen für die Einführung einer solchen Technologie. Im aktuellen Szenario wird eine Netzwerkumgebung aufgebaut, welche aus 3 Servern und beliebig vielen Benutzergeräten besteht. Alle Netzwerkteilnehmer sind dabei über einen Switch miteinander verbunden. Zu Beginn werden die Studenten angeleitet, bereits

erworbenes Wissen anzuwenden, indem sie Server 1 als DHCP-Server konfigurieren. Dabei wird der Umgang mit diesem Dienst und IPv4-Adressierungen wiederholt angewandt und somit gefestigt. In einem fortführenden Schritt wird sich ein Überblick über die von Packet Tracer zur Verfügung gestellte DNS-Oberfläche verschafft. Als DNS-Server dient hier Server 2. An dieser Stelle werden IP-Adressen und die dazugehörigen Namen in einer Tabelle gespeichert, damit diese auf Anfrage untereinander aufgelöst werden können (Abbildung 4.8).

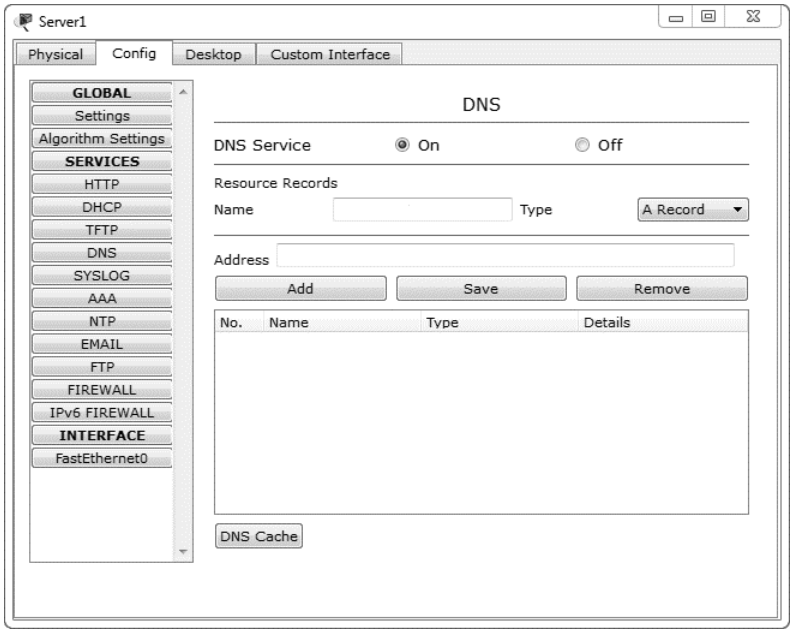

Abbildung 4.8, DNS-Konfigurationsoberfläche

Der Sachverhalt, dass an dieser Stelle noch keine Eintragungen vorgenommen werden können, soll den Studenten verdeutlichen, dass zuerst eine, zu einem Server zugehörige IP-Adresse vorhanden sein muss, die in einen Namen aufgelöst werden kann. In diesem Beispiel wird dazu praxisnah ein Webserver eingerichtet, welcher mittels HTTP eine Webseite (hier am Beispiel www.hs-mittweida.de) in den vorinstallierten Webbrowser eines PCs im Szenario lädt. Hierfür wird Server 3 verwendet. Die Einstellungen beschränken sich jedoch auf das Vergeben einer zum Netz passenden IP-Adresse. HTTP ist standardmäßig aktiviert. Zu anschaulichen Zwecken ist dem Bearbeiter ein HTML Code vorgegeben, welcher die später aufzurufende Webseite anschaulich gestaltet. Nach Abschluss der Konfiguration werden die Studenten aufgefordert, über den Webbrowser eines PCs die

Internetseite www.hs-mittweida.de zu öffnen. Da jedoch noch kein Eintrag in der Namenstabelle des DNS-Servers zu diesem vorhanden ist, kommt es zu keiner Anzeige, was wiederum zu dem Lerneffekt führt, dass DNS nur funktionieren kann, wenn ein entsprechender Eintrag auf dem verantwortlichen DNS-Server vorliegt. Dieser Eintrag wird im folgenden Schritt angelegt, indem die an den Webserver vergebene IP-Adresse mit www.hs-mittweida.de verknüpft und in die Namenstabelle des DNS-Servers eingetragen wird (Abbildung 4.9).

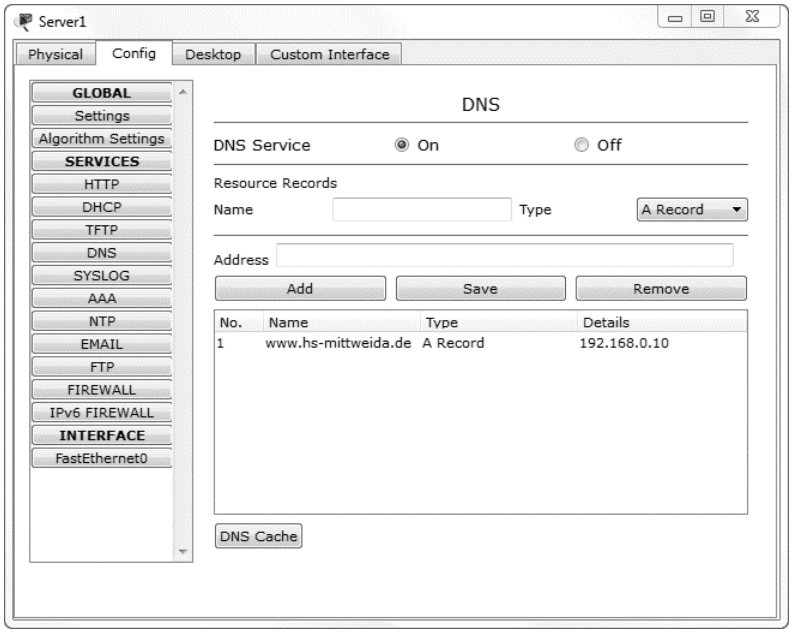

Abbildung 4.9, Eintrag in der DNS-Namenstabelle

Im Anschluss daran wird die eben aufgerufene Webseite aktualisiert. Durch den zuvor festgelegten Eintrag arbeitet die Auflösung zwischen IP-Adresse und entsprechendem Name korrekt und die Seite wird dargestellt. Um einen genaueren Einblick in die Übertragungen, beginnend beim Absenden des Befehls im Browser bis hin zur eigentlichen Darstellung der Seite, zu erhalten, weist die Versuchsanleitung an, eben diesen Vorgang im Simulationsmodus zu betrachten. Dadurch werden neue Kenntnisse hervorgebracht, wodurch in Verbindung mit der Anwendung von bereits vorhandenem Wissen der Lernprozess fortgeführt wird.

In Teilaufgabe 3 wird ein einfacher Mailserver konfiguriert, welcher den Studenten die grundlegende Arbeitsweise des heutigen Emailverkehrs aufzeigt. Dabei wird ebenfalls auf die für den Emaildienst wesentlichen Protokolle POP3 und SMTP

eingegangen, welche in allen aktuellen Email-Clients implementiert sind. Erneut besteht der erste Schritt darin, eine Netzwerkumgebung einzurichten, welche zu einem Teil aus Clients (PCs, Laptops usw.), zum anderen Teil aus einem Server (hier: Mailserver) besteht. Die dabei einzugebenden Netzwerkkonfigurationen müssen die Studenten erneut selbstständig vornehmen. Weiter im Versuch folgt die Einrichtung des Emailservers. Dabei müssen neben einer Domain für diesen Mailserver ebenfalls Benutzer angelegt werden. Wie in der Praxis werden Benutzername und Passwort verknüpft und auf dem Server abgelegt. Damit wird ein Verständnis dafür geschaffen, wo Benutzerdaten in der Praxis gespeichert werden. Die Software Packet Tracer stellt unter jedem Benutzerendgerät (PC, Laptop, Smartdevice usw.) einen Email-Client zur Verfügung, welcher nun an die eben vorgenommene Konfiguration angepasst wird, um die Kommunikation zwischen zwei Clients via Email zu ermöglichen (Abbildung 4.10).

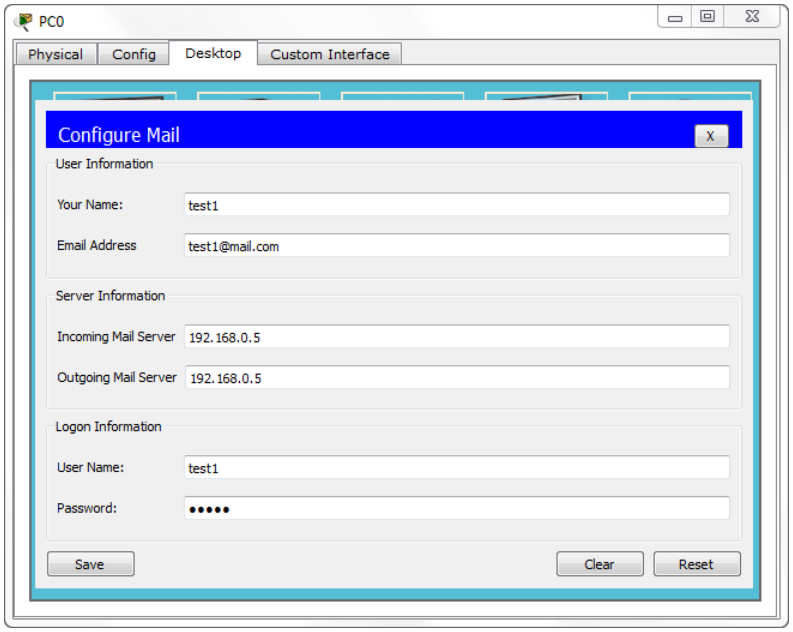

Abbildung 4.10, Konfigurationsfenster des Email-Clients

Nach Abschluss dieser Konfiguration auf mindestens zwei Rechnern können jetzt Emails gesendet und empfangen werden. Im Simulationsmodus des Programmes sind nun SMTP und POP3 Pakete detailliert verfolg- und analysierbar. Hierdurch werden die Funktionsweisen eines der wichtigsten Dienste des Internets, die beteiligten Protokolle und die damit verbundenen Transportwege der einzelnen

Datenpakete (z.B. Senden eines POP3 Pakets an den Mailserver bei Mailabholung) verständlich vermittelt.

In der 4. Teilaufgabe wird das Kollisionsverhalten innerhalb eines Netzwerkes simuliert und daran das in der parallel laufenden Vorlesung behandelte CSMA/CD Verfahren erläutert, welches vor der Einführung von Switches wesentlicher Bestandteil in der Netzwerktechnik war. Dazu wird von den Studenten zunächst ein einfaches Netzwerk eingerichtet, in welchem mehrere Endgeräte über einen Hub verbunden sind. Werden anschließend zwei einfache Übertragungen zeitgleich gestartet (im Beispiel: Ping), kommt es im Hub zur Kollision, was die Software anhand eines Flammensymbols visualisiert (Abbildung 4.11).

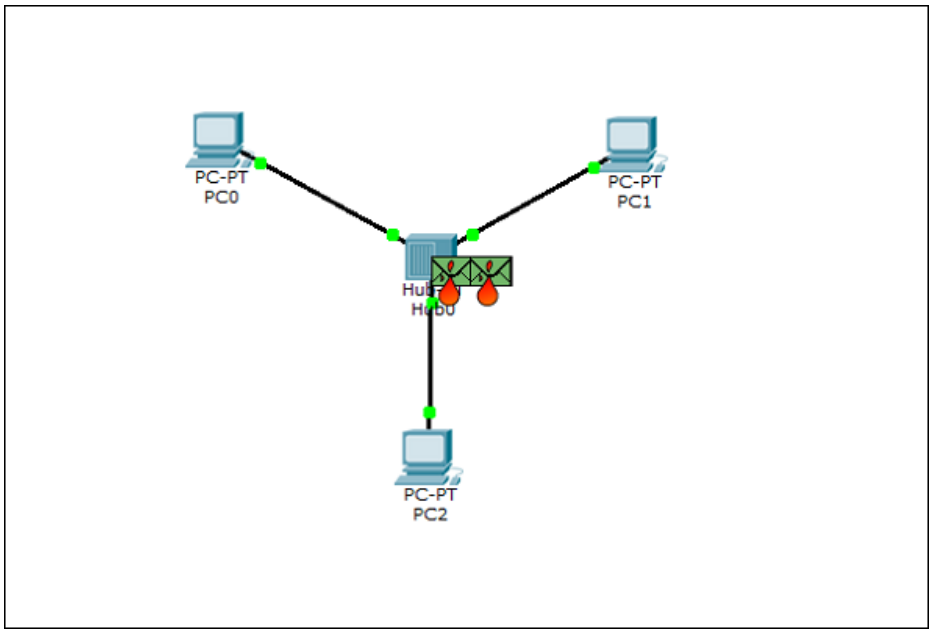

Abbildung 4.11, Kollision innerhalb des Netzwerkes

Die Übertragung kann in diesem Fall nicht abgeschlossen werden, was es offenkundig zu vermeiden gilt. An dieser Stelle wird dem Anwender in der Versuchsanleitung erläutert, dass genau aus diesem Grund CSMA/CD eingesetzt wurde. Durch dieses Verfahren konnte zwar den Kollisionen vorgebeugt werden, allerdings wirkte sich dessen Anwendung auch auf die Übertragungszeiten aus. Hier werden Parallelen zu Versuch 1 gezogen und weitere Gründe erläutert, weshalb Hubs in der Praxis nahezu vollständig durch Switches abgelöst wurden. Durch Ersetzen des Hubs mit einem Switch und erneutes Starten zweier Übertragungen

gleichzeitig wird ersichtlich, dass bei Verwendung von Switches keinerlei Probleme entstehen und somit die Vorteile dieser Geräte noch einmal verdeutlicht werden (Abbildung 4.12).

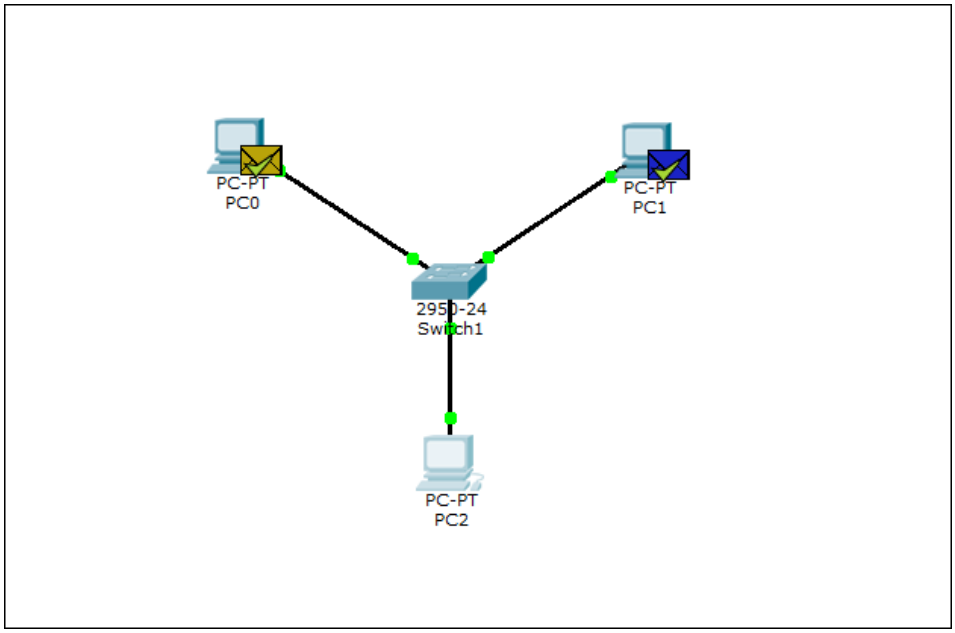

Abbildung 4.12, Keine Kollision bei Verwendung eines Switches

Teilaufgabe 5 bildet den Abschluss des zweiten Versuchs und führt in die Thematik des Routings ein. Bisher wurde im Praktikum lediglich mit einem Netz gearbeitet, da dies für das grundlegende Verstehen eines Sachverhaltes ausreichend ist. Jedoch existieren in der Praxis unzählig viele unterschiedliche Netze, welche in der Lage sein müssen, miteinander zu kommunizieren. Diese Aufgabe übernehmen Router. Im Rahmen dieser Aufgabe richten die Studenten ein Netzwerk ein, welches aus zwei Teilnetzen besteht. Diese werden zunächst lediglich über einen Switch miteinander verknüpft und der Anwender dazu aufgefordert, einen Kommunikationsversuch mittels Ping von Teilnetz A in Teilnetz B zu unternehmen. Ohne eine Möglichkeit zur Vermittlung kann diese Übertragung jedoch nicht funktionieren, das Paket wird verworfen. Dies wird in der Detailansicht der Übertragung noch einmal erläutert. Daraufhin wird ein Router zwischen die beiden Teilnetze geschaltet. Die Routerports, an denen die Teilnetze angeschlossen sind, erhalten nun ebenfalls eine IP-Konfiguration, passend zu dem jeweils verbundenen Teilnetz. Dieser Anschluss bildet das Default Gateway für das jeweilige Netz und

muss dementsprechend in die IP-Konfiguration der Netzteilnehmer mit aufgenommen werden. Leiten die Studenten nun eine erneute Übertragung von Teilnetz A nach Teilnetz B ein, ist diese erfolgreich. In der Detailansicht der Paketübertragung ist deutlich zu erkennen, wie bei einer Kommunikation innerhalb zweier unterschiedlicher Netze vorgegangen wird (Abbildung 4.13).

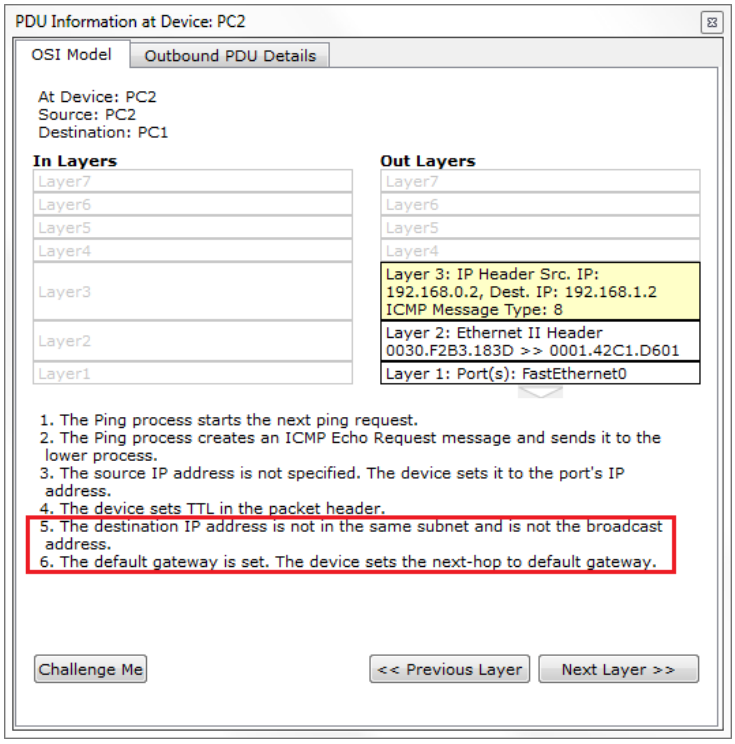

Abbildung 4.13, Detailansicht einer Dateiübertragung in unterschiedlichen Netzen

Wird bei einer Übertragung festgestellt, dass sich die Ziel-IP in einem anderen Netz befindet, werden die zu übertragenden Daten zunächst an das zugehörige Gateway geleitet, welches dann diese Daten anhand von Informationen aus Schicht 3 des OSI-Modells in das entsprechende Netz übermittelt. Die genaue Betrachtung der Paketübertragungen und deren Detailansichten im Simulationsmodus gewähren den Lernenden einen genauen Einblick in die Funktions- und Arbeitsweise von Routern.

Lösungsansätze zu Versuch 2

In Teilaufgabe 1 von Versuch 2 wird die DHCP-Technologie implementiert und der Anwender wird angewiesen, eine passende Start-IP und eine dazu passende Subnetzmaske anzugeben. Es kann beispielsweise die Konstellation 192.168.0.1

– 255.255.255.0 verwendet werden. Im nächsten Schritt wird dem Server eine zu dem DHCP-Pool passende IP-Adresse zugewiesen. Eine zu diesem Lösungsansatz passende Adresse könnte 192.168.0.254 lauten. Dies kann auf die unter Teilaufgabe 2 einzurichtende DHCP-Konfiguration übertragen werden. In diesem Fall kann dem DNS-Server zum Beispiel die IP 192.168.0.10 (Subnetzmaske 255.255.255.0) zugeordnet werden. Die vorgeschlagenen Konfigurationen können sich auch auf die Mailservereinrichtung unter Teilaufgabe 3, sowie auf das Netzwerk von Teilaufgabe 4 anwenden. Ebenfalls könnten IP-Adressen der Form 172.16.0.x (x steht hier für eine beliebige Ziffer zwischen 1 und 254) und der Subnetzmaske 255.255.0.0 verwendet werden. Teilaufgabe 5 basiert auf zwei unterschiedlichen Netzen. Um diese zu realisieren, könnte Netz 1 beispielsweise IP-Adressen der Form 192.168.0.x /24, Netz 2 IP-Adressen der Form 192.168.1x /24 erhalten. Dementsprechend muss der Routerport, an welchen Netz 1 angebunden ist, eine IP-Adresse der Art 192.168.0.x /24 erhalten, z.B. 192.168.0.254. Gegenübergestellt erhält der Port, welcher Netz 2 anbindet, eine IP-Adresse nach dem Schema 192.168.1.x /24, beispielsweise 192.168.1.254 (Subnetzmaske 255.255.255.0).

Lösungen zu den Aufgaben am Ende des Versuches:

1. Was bedeutet DHCP und wofür wird es benötigt?

DHCP (Dynamic Host Configuration Protocol) ist ein Protokoll, welches die automatische Zuweisung von Netzwerkkonfigurationen an einen Client durch einen Server ermöglicht.

2. Wie funktioniert ein DNS – Server?

Auf einem DNS-Server ist der gleichnamige Dienst DNS (Domain Name System) implementiert, welcher zur Namensauflösung dient. Auf diesem Server sind eine Reihe IP-Adressen mit dazugehörigen Namen verknüpft. Auf Anfrage löst dieser Server einen Namen in die entsprechende IP-Adresse auf und führt zum richtigen Server weiter.

3. Was ist die Aufgabe eines Routers?

Router dienen zur Weiterleitung von Datenpaketen zwischen unterschiedlichen Netzen. Der Vorgang, in welchem ein Paket von einem Netz in ein anderes geleitet wird, heißt Routing.

4. Wofür ist das Address Resolution Protocol in IPv4-Netzwerken zuständig?

Bei IPv4-Adressierungen wird das ARP-Protokoll zur Ermittlung der MAC-Adresse anhand der IP-Adresse eingesetzt. Diese Verbindungen trägt das Protokoll folgend in die ARP-Tabellen der beteiligten Rechner ein.

4.5.3 Versuch 3

Versuch 3 baut auf den theoretischen Grundlagen von Versuch 1 und Versuch 2 auf und verleiht diesen einen praxisnahen Bezug. Die Bearbeitungszeit für diesen Versuch ist mit 180 Minuten veranschlagt. Der dritte Versuch gliedert sich ebenfalls in mehrere Teilaufgaben, welche die Studenten schrittweise abarbeiten. Dabei werden grundlegende Vorgehensweisen und bekannte theoretische Prinzipien nicht mehr sukzessive erläutert, um bereits erworbenes Wissen vom Anwender zu festigen. Während des Versuches werden den Studenten fortführend Hinweise gegeben, in welchem unmittelbaren Bereich die behandelte Technologie eingesetzt wird, um stets den Bezug zur Praxis zu wahren. Dieser Versuch beschäftigt sich erstmals auch mit der Routerkonfiguration via IOS Command Line Interface, wie es in der Praxis bei der Verwendung von Cisco Routern üblich ist. Weiterhin bereitet er das in Versuch 1 und 2 erlangte Wissen auf, unterstützt jedoch die Studenten zusätzlich mit detaillierten Anweisungen, um in die neuen Thematiken einzuführen.

In Teilaufgabe 1 wird ein einfaches MAN simuliert, um aufzuzeigen, wie verknüpfte Netzwerke über einen ausgedehnteren geografischen Raum arbeiten. Dabei wird das Netzwerk der Hochschule Mittweida als Praxisbeispiel herangezogen, da mehrere Standorte innerhalb einer Stadt in einem Netzwerk liegen. Als weiteres Beispiel werden Firmenfilialen genannt, welche ebenfalls innerhalb eines Ortes miteinander verknüpft sind. In einem ersten Schritt richten die Studenten 3 Teilnetze, bestehend aus jeweils zwei PCs und einem Switch, ein. Diese Netze sind jeweils an einen Router angebunden, welcher die Verbindungsmöglichkeit nach außen bildet. Diese Router gilt es über deren serielle Ports mit einem entsprechenden Kabel miteinander zu verbinden. Diese Technik eignet sich für die Verbindung mehrere Standorte untereinander und wird deshalb in diesem Beispiel eingesetzt. Die angebundenen PCs repräsentieren hier sämtliche Netzteilnehmer des jeweiligen Ortes. Die Versuchsanleitung weist an, dass sich alle Teilnetze in unterschiedlichen Netzen befinden sollen. Die statische IP-Vergabe in Netzen dieser Größe ist in der Praxis unüblich und findet aus diesem Grund im erläuterten Praktikumsversuch dynamisch (DHCP) statt, was den Anwendern wiederholt vermittelt, wie in einem praktischen Umfeld verfahren wird. Diesen Dienst implementieren die Studenten mit Hilfe des Command Line Interfaces. Dies führt die Praktikanten an diese Art der Konfiguration heran und macht sie mit diesem Interface und den dazugehörigen Konsolenbefehlen vertraut, da es durch die Markstellung von Cisco Systems wahrscheinlich ist, damit in Verbindung zu kommen. Da das Hauptaugenmerk des Praktikums jedoch darauf liegt, den Anwender mit den wichtigsten Netzwerktechnologien vertraut zu machen, beschränkt sich die Verwendung der Konsole auf grundlegende Anwendungen.

In den nächsten Schritten erläutert die Versuchsanleitung die Implementierung eines DHCP-Dienstes auf einem der Router. Dies gilt es anschließend auf den beiden anderen Routern zu wiederholen, um zu gewährleisten, dass sämtliche Netzteilnehmer der einzelnen Netze ihre Netzwerkkonfigurationen mittels DHCP automatisch zugewiesen bekommen. Ist die Einrichtung abgeschlossen, folgt ein Test auf fehlerfreies Arbeiten des DHCP-Dienstes. Im Folgenden wird sich der Kommunikation der Router untereinander zugewandt. Theoretisch wurde dies bereits in Versuch 2 abgehandelt, wodurch es den Studenten demzufolge leichter fällt, die entsprechenden Einstellungen vorzunehmen. Als Hilfestellung findet sich

in der Versuchsbeschreibung eine Tabelle, welche die zu verwendenden IP-Konfigurationen bereitstellt. Um zu demonstrieren, dass zu diesem Zeitpunkt noch keine Übertragung stattfinden kann, ordnet die Versuchsanleitung an, eine Dateiübertragung von einem Netz in ein anderes einzuleiten. Da die Netzwerke an dieser Stelle nicht direkt miteinander verbunden sind, benötigen die Router Einträge in deren Routingtabellen, um zu übermittelnde Daten korrekt zu übertragen. Dabei wird jedem, sich in Verwendung befindlichen Port eines Routers eine IP-Route zugewiesen, welche auf das jeweils angebundene Netz verweist, um eine Kommunikation zu ermöglichen. Dies geschieht hier über statische Routen in der Konfigurationsoberfläche der Router (Abbildung 4.14).

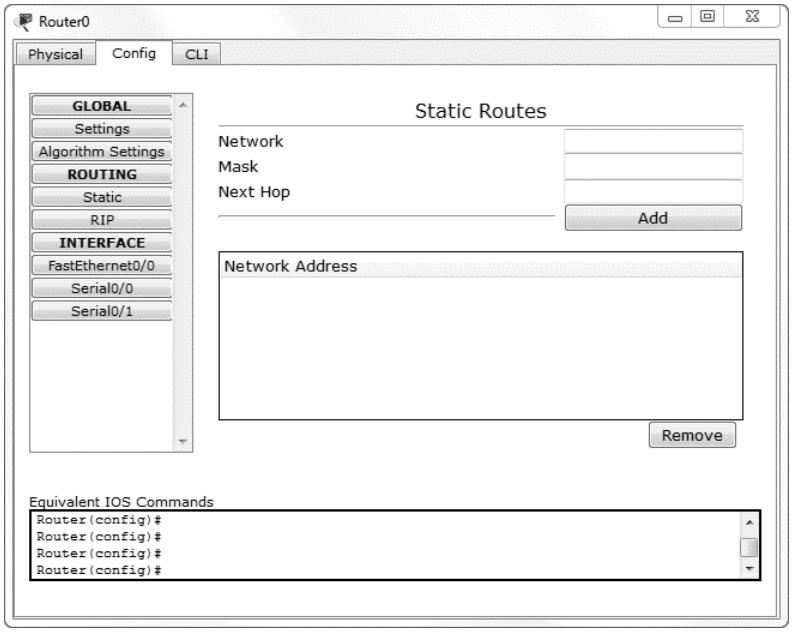

Abbildung 4.14, Routingtabelle eines Routers in Packet Tracer

In diese Tabelle werden die Daten des zu kontaktierenden Netzes, sowie der nächste Netzknoten, an welchen ein zu übertragendes Paket vermittelt werden muss (Next Hop, an dieser Stelle der entsprechende serielle Port des Routers von Teilnetz A, über welchen der Router von Teilnetz B angebunden ist usw.) eingetragen. Wurden alle Einstellungen erfolgreich durchgeführt, kann die Funktionsweise des eingerichteten Netzwerkes im Simulationsmodus getestet werden. Die Studenten senden ein einfaches Datenpaket von Teilnetz A in

beispielsweise Teilnetz B und betrachten die Detailinformationen, welche Packet Tracer zur Verfügung stellt (Abbildung 4.15).

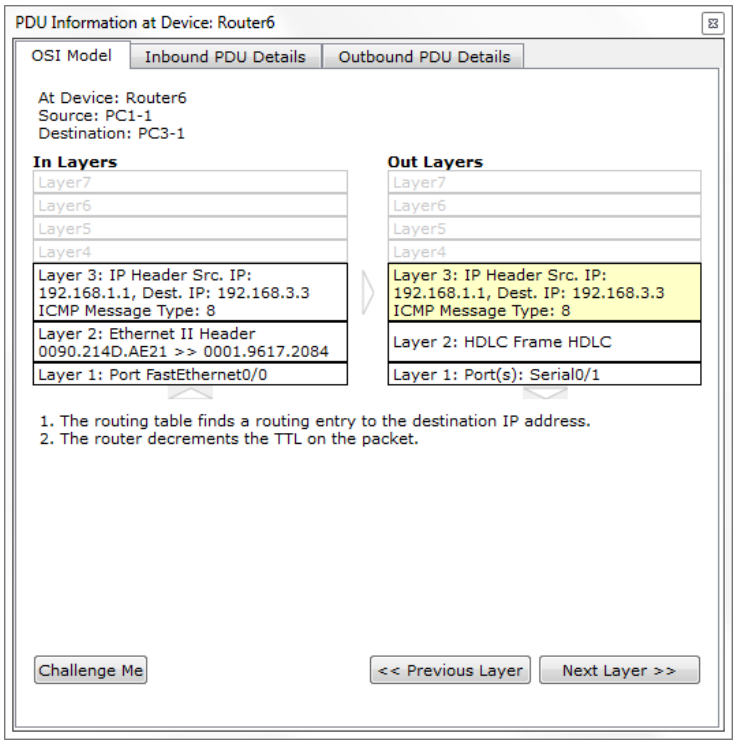

Abbildung 4.15, Detailansicht Routing

Diese Detailansicht zeigt dem Anwender auf, dass der Router die eigene Routingtabelle nach Einträgen durchsucht, welche mit den Paketinformationen übereinstimmen. Wird ein passender Eintrag gefunden, wird das Paket ordnungsgemäß übermittelt. Eine abschließende Grafik zeigt den Studenten erneut, wie die zuvor behandelte Technologie in der Praxis Anwendung finden könnte (Abbildung 4.16).

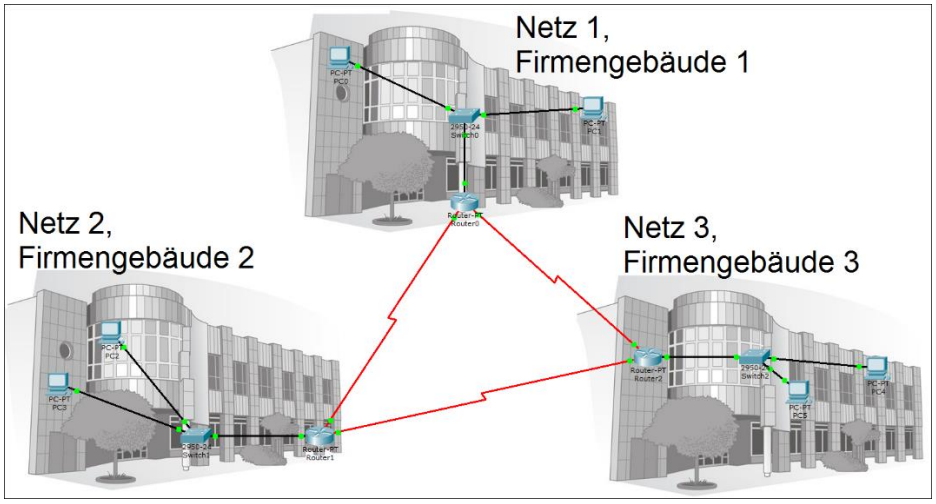

Abbildung 4.16, Grafische Darstellung zum Praxisverständnis

Die zweite Aufgabe dieses Versuches geht auf die Thematik VLAN ein. In der Praxis finden sich verschiedene Arten von VLANs. Der Versuch beschränkt sich auf statische VLANs, bei denen die Zugehörigkeiten von einem Administrator manuell festgelegt werden. Dies macht den Anwender mit der Arbeitsweise von VLANs vertraut und zeigt ihm praktische Einsatzmöglichkeiten auf. Zunächst wird die Netzwerkumgebung eingerichtet, in welcher diese Teilaufgabe ihre Anwendung findet. Dabei kommen mehrere PCs zum Einsatz, welche in einem ersten Schritt über einen Switch verbunden sind (Abbildung 4.17).

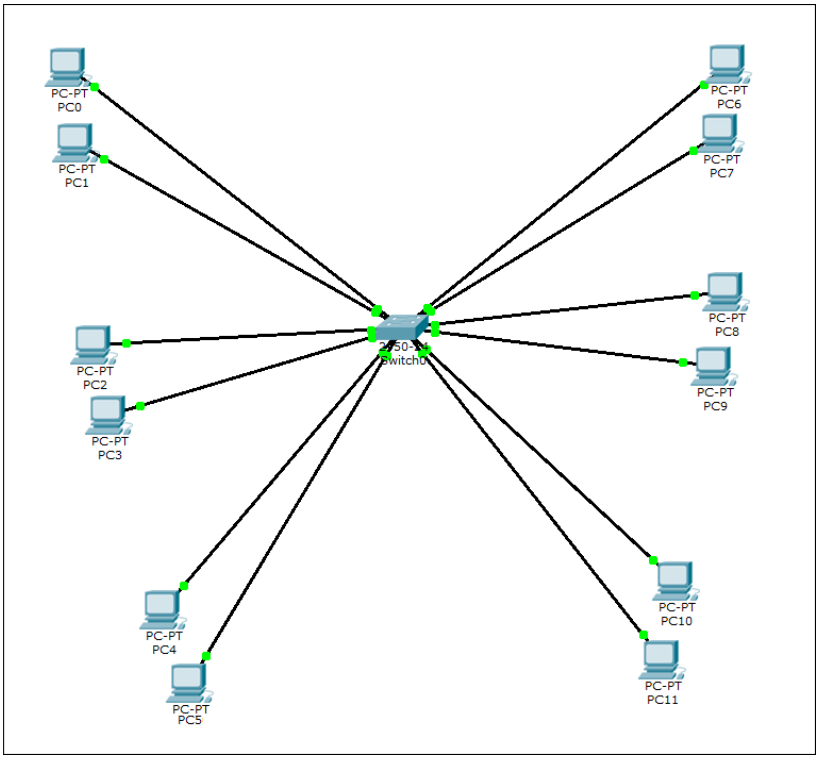

Abbildung 4.17, VLAN Aufbau, 1 Switch

Über die Konfigurationsoberfläche des Switches können nun verschiedene VLANs eingerichtet werden. In diesem Beispiel soll mit 3 VLANs gearbeitet werden, welche der Anwender selbstständig anlegt. In der Praxis werden diese Switches ebenfalls über die Konsole programmiert. Davon soll in diesem Versuch abgesehen werden, da das Verstehen der Funktionsweise eines VLANs im Vordergrund steht. Auf Grund dessen werden die Einstellungen in der grafischen Oberfläche des Switches vorgenommen, welche von Packet Tracer zur Verfügung gestellt wird. Zunächst werden VLAN 10, 20 und 30 zur VLAN Datenbank hinzugefügt. In der Praxis entspricht dies dem Einrichten der einzelnen VLANs durch den Administrator (Abbildung 4.18).

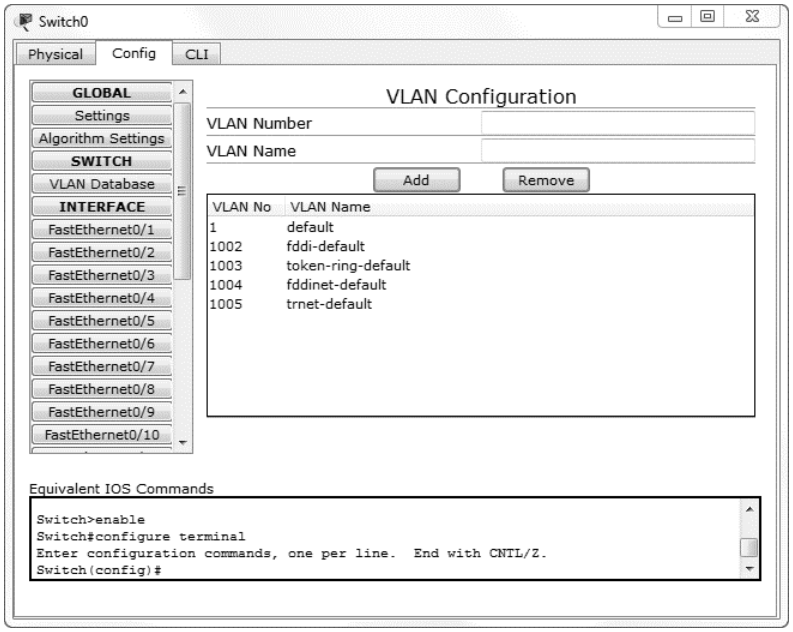

Abbildung 4.18, VLAN-Konfigurationsoberfläche

In einem nächsten Schritt legen die Studenten fest, welche Ports des Switches welchem VLAN zugeordnet sind. Im Beispiel werden dabei jeweils 4 PCs einem VLAN zugewiesen. An die Konfiguration anschließend sendet der Anwender mehrere Datenpakete zwischen den beteiligten Rechnern. Nur jene PCs, welche sich im selben VLAN befinden, sind dazu in der Lage, miteinander zu kommunizieren. Dies hilft den Studenten, das Prinzip hinter dieser Technologie zu verstehen. Aufbauend auf dieses Beispiel wird den Studierenden der Einsatz von Trunks erläutert. Dazu wird ein weiterer Switch in das Szenario eingebracht und mit den gleichen Parametern konfiguriert wie der bereits Vorhandene. Es folgt die Anbindung von jeweils zwei PCs eines jeden Netzes an den neuen Switch mit der Ausstattung der entsprechenden VLANs. Die nun folgende Verbindung der beiden Switches wird als Trunk eingerichtet. Dies geschieht im Konfigurationsfenster des jeweiligen Ports (im Beispiel wurde der Port FastEthernet0/24 auf beiden Switches für den Trunk reserviert). Dieser Trunk vereint alle VLANs in einer logischen Verbindung, was dem Anwender das Prinzip des Trunking verdeutlicht. Im Versuch wird als Praxisvergleich die Vernetzung mehrerer VLANs innerhalb eines Gebäudes über mehrere Stockwerke angeführt. Abschließend wird eine erneute Datenübertragung initiiert. Ein Blick auf die Detailansicht des Paketes zeigt, dass der Switch auf Grund des Ports, auf welchem das Datenpaket eingeht, das

zugehörige VLAN identifizieren kann. Ist dieses auf dem Trunk zugelassen, wird das Paket fehlerfrei weitergeleitet (Abbildung 4.19).

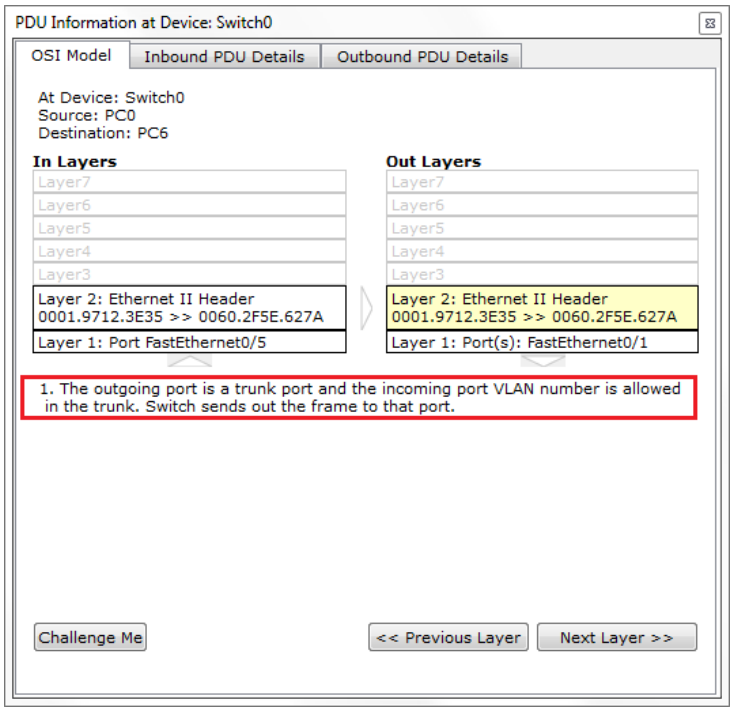

Abbildung 4.19, Detailansicht VLAN-Trunk

Teilaufgabe 3 des Versuchs impliziert die Arbeitsweise einer Firewall, welche serverseitig in einem überschaubaren Netzwerk implementiert wird. Außerdem wird in dieser Aufgabe an ausgewählten Beispielen der Zusammenhang zwischen Protokollen und Diensten erläutert. Zunächst wird das Versuchsszenario eingerichtet, bestehend aus PCs, Switch, Router und Server. Im Anschluss daran nehmen die Studenten sämtliche Netzwerkkonfigurationen vor, welche für eine Kommunikation zwischen Client und Server erforderlich ist. Die ständige Wiederholung solcher Einrichtungen in unterschiedlichen Szenarien trägt dazu bei, die Vorgehensweisen und theoretischen Prinzipien beim Anwender nachhaltig zu festigen. Des Weiteren werden die Bearbeiter angeleitet, die Dienste HTTP, DNS und FTP auf dem Server zu konfigurieren und zu aktivieren, um diese später in den Test der Firewall mit einzubeziehen. Sind die Grundeinstellungen abgeschlossen, wird die Kommunikationsfähigkeit aller beteiligten Netzwerkkomponenten untereinander mittels geeigneter Datenpakete getestet. Ist diese gewährleistet, folgt die Konfiguration der Firewall, welche im entsprechenden Bereich auf dem Server vorgenommen wird. An dieser Stelle wird nun festgelegt, wie mit bestimmten

Protokollen verfahren wird. Im Versuch wird der Anwender mit Hilfe einer Tabelle angewiesen, welche Einstellungen vorgenommen werden müssen. Die Firewall arbeitet paketbasiert, was bedeutet, dass nur bestimmte Protokolle auf Zulassung überprüft werden. In der Praxis wurden bestimmte Ports für entsprechende Protokolle standardisiert, was den Studenten durch einen Verweis in der Versuchsanleitung vermittelt wird. Diese Ports gilt es ebenfalls in der Konfigurationsoberfläche der Firewall anzugeben, damit diese ordnungsgemäß arbeiten kann. Sind alle Regeln festgelegt, geht die Versuchsanleitung in den Test über. Dabei werden im Simulationsmodus Paketübertragungen gestartet. Im Paketfilter werden jene Pakete angewählt, welche es zu betrachten gilt (im Beispiel ICMP, HTTP und FTP). Durch Aufrufen der Detailansicht des Sendevorgangs wird deutlich, wie und insbesondere auf welcher Schicht des OSI-Modells (hier: Schicht 3, da paketbasiert) die Firewall arbeitet (Abbildung 4.20).

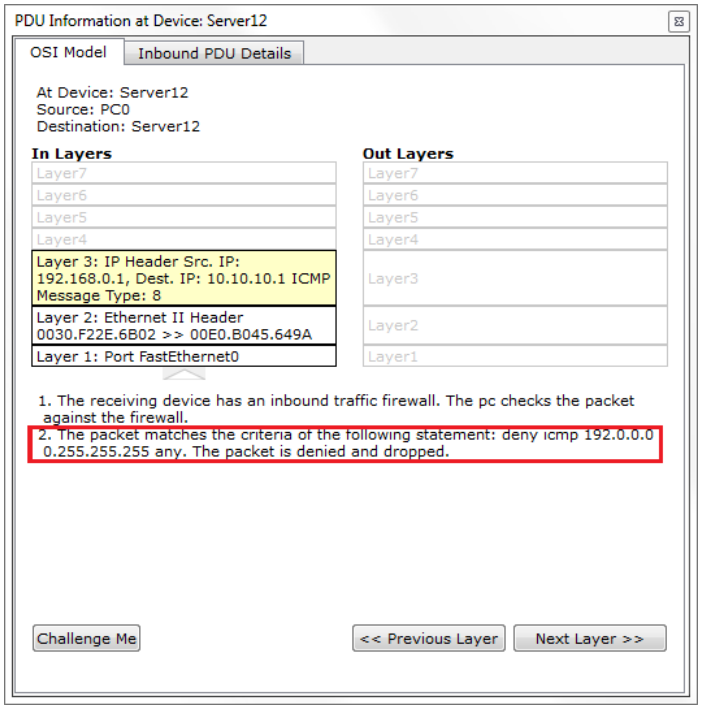

Abbildung 4.20, Detailansicht eines blockierten Datenpakets

Diese Detailansicht zeigt zum Beispiel die Blockierung eines ICMP-Datenpakets.

Es wird den Studenten verdeutlicht, dass, sobald ein Datenpaket den Server erreicht, eben jenes durch dessen Firewall blockiert und verworfen wird, da es gegen die zuvor festgelegten Richtlinien verstößt. Die Aufgabe demonstriert diesen Sachverhalt mit zwei weiteren Beispielen (FTP, HTTP), um den Anwender beim Verstehen dieses Prinzips zu unterstützen.

Unter Teilaufgabe 4 des dritten Versuchs wird mit NAT eine wesentliche und praxisrelevante Technologie behandelt. Diese wird nahezu in allen Bereichen der Netzwerktechnik eingesetzt, weshalb es von großer Bedeutung ist, das Prinzip hinter NAT zu verstehen und die Einsatzgebiete zu kennen. Zu Beginn richtet sich der Anwender ein übersichtliches Netzwerk ein, bestehend aus PCs (vgl. Heimanwender), welches über einen Router nach außen kommuniziert. An diese Konstellation ist ein Server über einen weiteren Router angebunden (vgl. Anbieter eines Dienstes). Die grundlegende Netzwerkkonfiguration erfolgt in einem nächsten Schritt durch den Anwender, wobei zahlreiche, bereits erworbene Kenntnisse zum Einsatz kommen. Ist dies abgeschlossen, wird die NAT-Technologie mit Hilfe des Command Line Interfaces auf den Routern implementiert. Dies ist Schritt für Schritt in der Versuchsanleitung dokumentiert.

Im Anschluss daran wird die Arbeitsweise des zu untersuchenden NAT-Verfahrens im Simulationsmodus analysiert. Dabei wird ein einfaches ICMP-Paket von einem der PCs an den Server gesendet. Die IP-Informationen dieses Rechners werden im Router in nach außen gültige IP-Konfigurationen übersetzt. Dieses Verfahren wird in jedem privaten Haushalt angewandt, wodurch der entsprechende Benutzer nach außen nur durch eine öffentlich zur Verfügung gestellte IP auftritt. Dies wird den Studenten mit einem Blick in die Detailansicht eines Datenpakets dargelegt. Ruft man die Spalte der ausgehenden Informationen auf, wird ersichtlich, dass die privaten IPs der PCs (SRC IP) durch die implementierte NAT Technologie in die öffentlich gültige IP des Routers übersetzt wurde (Abbildung 4.21).

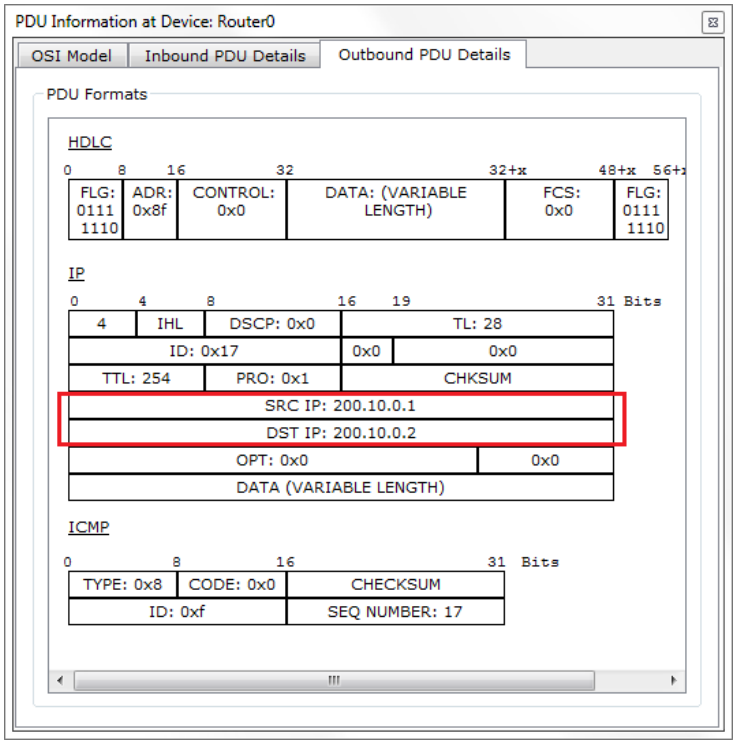

Abbildung 4.21 Ausgehende Paketinformationen

In der Praxis wird eine NAT Übersetzung erwartungsgemäß nicht für jedes Gerät einzeln realisiert, sondern darauf programmiert, dass jede private IP in dem angeschlossenen Netz übersetzt wird, welche versucht nach außen hin zu kommunizieren. Der weiterführende Teil dieser Teilaufgabe demonstriert diesen Sachverhalt, indem der Anwender eine Access List anlegt, in welcher sämtliche Netzteilnehmer erfasst sind, welche einer Übersetzung bedürfen. Dies erweitert zusätzlich die Wirklichkeitsnähe dieses Versuches.

Die letzte Teilaufgabe des dritten Praktikumsversuchs thematisiert die IPv6-Technologie. Ein einleitender Satz verweist noch einmal auf das vorhergehend behandelte NAT-Verfahren, welches einen großen Beitrag zur Verzögerung der Erschöpfung der IPv4-Adressen beigetragen hat und erläutert damit die Grundidee hinter der Technologie. Da NAT allerdings auch problembehaftet ist und die Erschöpfung des IPv4-Adressenkontingents nicht stoppen, sondern nur verzögern kann, wurde IPv6 als Nachfolger zu IPv4 entwickelt. Diese Aufgabe lässt die Studenten ein Netzwerkszenario einrichten, welches komplett auf IPv6 basiert, um ihnen ein Verständnis für dieses Adressierungsprinzip zu vermitteln. In einem ersten Schritt wird das Netzwerk mit seinen Grundkomponenten aufgebaut. In diesem

Beispiel wird sich dabei auf PCs, Switches und einen Router beschränkt, da dies für den Aufbau eines Grundverständnisses für das IPv6-Prinzip ausreichend ist. Anschließend an die Einrichtung des Netzwerkes folgt die Konfiguration des Routers auf IPv6. Dies erfolgt über das CLI und ist in der Versuchsanleitung schrittweise erläutert. Dabei wird dem Port, an welchen Netz 1 angebunden ist, eine Link-Local Adresse (im Beispiel FE80::1, verkürzte Schreibweise) zugewiesen. Um ein Routing zu ermöglichen, benötigt der für Netz 2 verantwortliche Port ebenfalls eine solche Adresse. Auf Grund des IPv6-Prinzips und der rein lokalen Signifikanz einer solchen Link-Local Adresse kann dieser Port dieselbe Adresse erhalten, wie jener Port, welcher mit Netz 1 verbunden ist. Diese Adressen ermöglichen jedoch noch keine Kommunikation, da diese nicht routingfähig sind. Sie fungieren lediglich als eine Art Äquivalent zu dem Default Gateway bei IPv4-basierten Netzwerken (IPv6 Gateway). Außerdem besitzen die Endgeräte ebenfalls noch keine IPv6-Adressen. In einem nächsten Schritt konfiguriert der Anwender globale Unicast-Adressen für beide Teilnetze, aus welchen die Endgeräte dann ihre IPv6-Adressen generieren. Dabei kommt für Teilnetz 1 die globale Unicast-Adresse 2001:A1:AAAA:A::1, für Teilnetz 2 2001:A1:AAAA:B::1 (jeweils verkürzte Schreibweise) zum Einsatz. Die Versuchsanleitung schlüsselt die verkürzten Schreibweisen zusätzlich in die vollständigen Schreibweisen auf, um so beide Darstellungsweisen zu zeigen und die Studenten damit vertraut zu machen. Die globalen Unicast-Adressen werden ebenfalls per Konsole konfiguriert. Nachdem diese Konfiguration abgeschlossen ist, wird die IP-Adressierungsoberfläche der Endgeräte aufgerufen und die Generierung der IPv6-Adressen eingeleitet. Anhand der generierten Adressen erkennt der Anwender, wie diese sich zusammensetzen, was ihm verdeutlichen soll, wie der IPv6-Mechanismus arbeitet. Durch die Angabe eines 64bit-Netzpräfix, bleiben 64bit der IPv6-Adress übrig. Dieser wird basierend auf der MAC-Adresse des entsprechenden Gerätes generiert, wie die Studenten anhand der Anzeige im Konfigurationsfenster erkennen können (Abbildung 4.22).

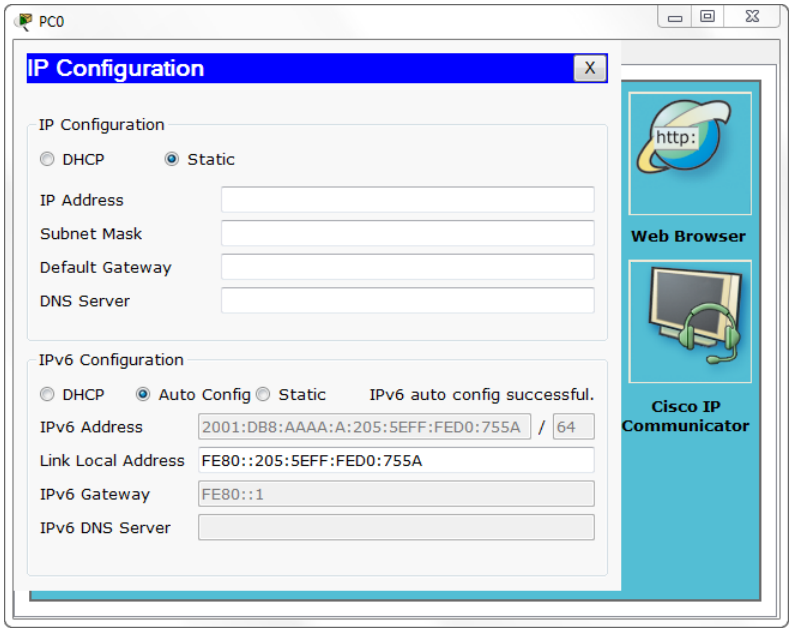

Abbildung 4.22, Generierte IPv6-Adresse, basierend auf Konfiguration und MAC-Adresse

Zum Abschluss wird das eingerichtete Netzwerk durch Übertragung eines IMCPv6-Daytenpakets (äquivalent zu ICMP bei IPv4) von einem Gerät aus Teilnetz 1 zu einem in Teilnetz 2. Diese wird nun schrittweise im Simulationsmodus vom Anwender verfolgt. Eine Betrachtung der Detailansicht dieses Pakets verdeutlicht, dass die Übertragung vollständig ohne die herkömmlichen IPv4-Adresskonfigurationen (IPv4-Adresse, Netzmaske usw.) durchgeführt wird und auch erfolgreich ist. Durch Aufrufen der ausgehenden Details des Pakets wird den Studenten zusätzlich offenbart, wie die IPv4 Parameter durch die IPv6 Konfiguration ersetzt wurden (Abbildung 4.23).

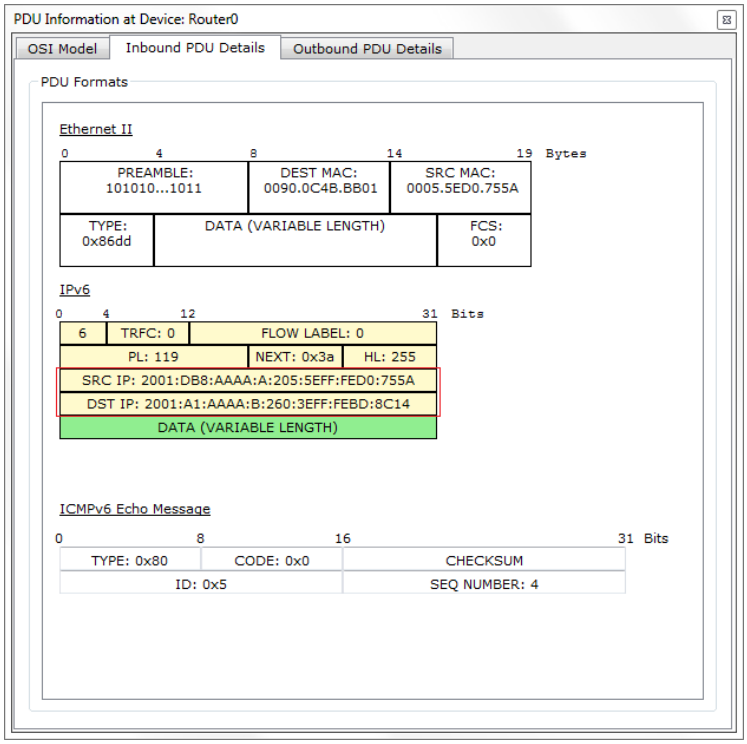

Abbildung 4.23, Detailansicht eines ICMPv6-Datenpakets

Lösungsansätze zu Versuch 3

Teilaufgabe 2 simuliert verschiedene VLANs innerhalb eines Netzwerkes. Alle 12 PCs könnten sich beispielsweise in einem 192.168.0.0 /24 Netz befinden.

Lösungen zu den Aufgaben am Ende des Versuches:

1. Von welcher Technologie stellt MAN eine Sonderform dar?

MAN (Metropolitan Area Network) stellt eine Sonderform der WAN (Wide Area Network)-Technologie dar.

2. Was bedeutet VLAN und wozu dient es?

VLAN steht für Virtual Local Area Network und dient der Aufteilung eines physikalischen Netzwerks in mehrere virtuelle Teilnetze.

3. Auf welcher Schicht des OSI – Modells arbeiten paketfilterbasierende Firewalls?

Paketbasierende Firewalls greifen auf Schicht 3 des OSI-Modells zu.

4. Wie funktioniert NAT und wozu wird es verwendet? Welche Nachteile hat es?

NAT (Network Address Translation) ist meistens auf Routern implementiert und ersetzt vorhandene Informationen der Netzwerkkonfiguration (z.B. private Heim-IP-Adressen in öffentliche, im Internet zugelassene IP-Adressen) mit anderen Werten. Dadurch erlaubt NAT jedoch keine Adressierung der Endgeräte.

5. Wo liegt der Unterschied zwischen IPv4 und IPv6 Adressierungen?

IPv4-Adressierungen benutzen 32-Bit-Adressen und werden in dezimaler Schreibweise dargestellt, während IPv6-Adressierungen Adressen 128 Bit nutzen und hexadezimal dargestellt werden. Dadurch ist der Adressbereich von IPv6 um ein vielfaches größer, als jener von IPv4.

4.5.4 Versuch 4

Versuch 4 bildet den Abschluss des Praktikums. Die Bearbeitungszeit beträgt 180 Minuten. Im Rahmen eines Komplexbeispiels wird das aus den vorhergehenden Versuchen generierte Wissen gefestigt und selbstständig auf ein vorgegebenes Szenario angewandt. Dabei realisieren die Studenten eine Umgebung, welche einen heimischen Internetzugang simuliert. Dabei werden sämtliche behandelte Technologien auf dieses praktische Beispiel übertragen, um alle erworbenen Kenntnisse weiter zu trainieren bzw. deren Anwendungssicherheit zu überprüfen. Durch dieses allumfassende Beispiel wird der Lernprozess abgerundet und eventuell entstandene Unklarheiten ausgeräumt. Der Versuch besteht aus dieser einen Aufgabe, welche in 5 Abschnitte unterteilt ist, welche zu einem Teil informativen, zum anderen Teil hilfestellenden Charakter besitzen. Dabei werden jedoch nur bis dahin unbekannte Vorgehensweisen mit der Packet Tracer Software erläutert. Alle weiteren Konfigurationen werden ohne Hilfestellungen durchgeführt.

Abschnitt 1, 2 und 3 erläutern die einzelnen Szenarien, welche die Studenten einrichten müssen, um anschließend das Komplettbeispiel vorliegen zu haben (Heimnetz 1 und 2, Servernetz). Unter Abschnitt 3 sind weiterhin alle Anforderungen aufgelistet, welche im Rahmen des Versuches umgesetzt werden sollen.

Diese Anforderungen lauten:

- Von den Endgeräten beider Heimnetze soll die Website www.hs-mittweida.de durch Eingabe der Domain über den Web Browser erreichbar sein.
- Ein Endgerät aus Heimnetz 1 soll via Email (xxx@hs-mittweida.de) mit einem Endgerät aus Heimnetz 2 und umgekehrt kommunizieren können.
- Nach außen sollen alle Endgeräte in den Heimnetzen unter derselben, für den betreffenden Anschluss öffentlich gültigen IP Adresse auftreten.

Abschnittsabschließend gibt die Anleitung vor, sämtliche Konfigurationen nun umzusetzen und alle Vorgaben zu implementieren. Dabei werden weiterführende Randinformationen zum allgemeinen Verständnis zur Verfügung gestellt.

Ist die gesamte Einrichtung abgeschlossen, wird in Abschnitt 4 die Verknüpfung zwischen Endbenutzer und Serviceanbieter schrittweise erläutert, da diese Vorgehensweise in früheren Versuchen noch nicht betrachtet wurde. Hat der Anwender das Komplettszenario umgesetzt, wird dieses auf Funktion sämtlicher gestellter Anforderungen getestet. Abschnitt 5 dient zur Information der Studenten, indem er grafisch darstellt, wie die in diesem Beispiel verwendeten Komponenten in der Realität geografisch angeordnet sein könnten. Dadurch erlangen die Studenten ein praktisch orientiertes Bild, welches sie unterstützt, kennengelernte Technologien auf die Praxis zu übertragen (Abbildung 4.24).

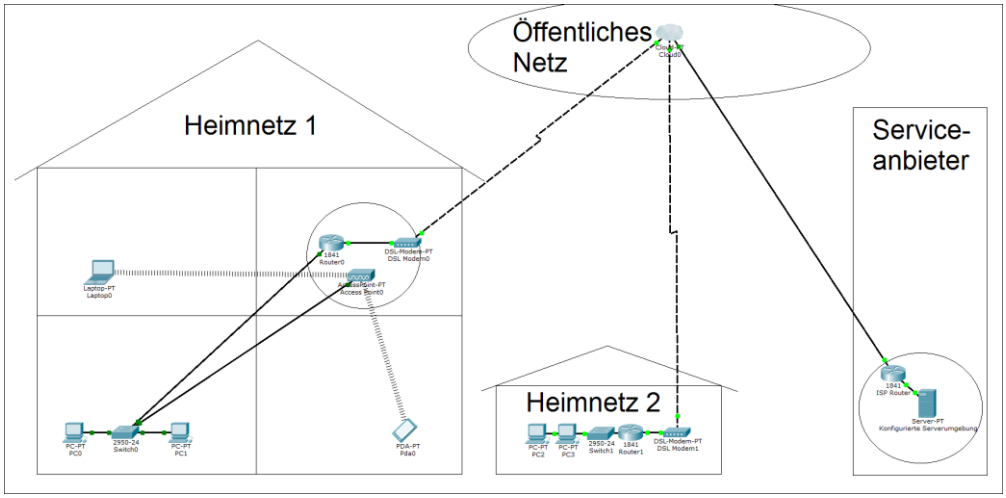

Abbildung 4.24, Geografische Beispielanordnung des Komplexszenarios

Lösungsansätze zu Versuch 4

Unter Abschnitt 1 wird zunächst Heimnetz 1 konfiguriert. Dazu sollen innerhalb des Netzes private IP-Adressen per DHCP an alle Endgeräte vergeben werden. Die DHCP-Konfiguration ist per CLI auf dem Router einzurichten (vgl. Versuch 3, Teilaufgabe 1). Heimnetz 1 kann zum Beispiel mit 192.168.0.0 /24 definiert werden. Das Default Gateway von Heimnetz 1 erhält dann praxisnah die IP-Adresse 192.168.0.1 /24. Ping stellt beispielsweise eine Möglichkeit zur Überprüfung der Kommunikationsfähigkeit der Geräte innerhalb von Heimnetz 1 dar. Als öffentliche IP des Routers wäre die Adresse 144.55.0.1 (Subnetzmaske 255.255.0.0) möglich (hierbei ist zu beachten, dass die öffentlichen Adressen der anderen Router in diesem Beispiel im selben Netz liegen müssen).

Heimnetz 2 unter Abschnitt 2 könnte beispielsweise mit dem Netz 192.168.1.0 /24 konfiguriert werden, mit der IP-Adresse 192.168.1.1 /24 als Default Gateway. Als öffentliche IP-Adresse des Routers von Heimnetz 2 könnte hier 144.55.0.2 /16 zum Einsatz kommen.

Unter Abschnitt 3 werden verschiedene Dienste implementiert. Dazu werden die Serverfunktionen Email, DNS und HTTP (Webserver) eingerichtet. Alle Server benötigen nun noch eine IP-Konfiguration. Dafür eignet sich beispielsweise 10.0.0.0 (Subnetzmaske 255.0.0.0). Dementsprechend kann das Default Gateway der Serverumgebung (ISP) die IP-Adresse 10.0.0.1 /8 erhalten. Nach außen könnte 144.55.0.3 /16 eingesetzt werden, basierend auf den in Abschnitt 1 und 2 vergebenen öffentlichen IPs. Damit alle Endgeräte unter der öffentliche IP eines zuständigen Routers auftreten, muss NAT auf den entsprechenden Routern konfiguriert werden, welches via CLI realisiert wird (vgl. Versuch 3, Teilaufgabe 4).

5 Zusammenfassung

5.1 Ergebnisse

Kernziel dieser Diplomarbeit ist die Entwicklung eines Praktikums für Studenten der Kommunikationstechnik, welches in die Grundlagen der Netzwerktechnik einführt und die Funktionsweisen verbreiteter Technologien auf diesem Gebiet vermittelt. Weiterführend wurde die Thematik der Netzwerksimulation einführend behandelt und aktuelle Softwarebeispiele gegenübergestellt. Weiterhin wurde die zu Grunde liegende Software Cisco Packet Tracer vorgestellt und analysiert.

Im Rahmen der Erarbeitung des Praktikums entstanden 4 Einzelversuche, welche an Studenten gerichtet ist, welche zu diesem Zeitpunkt noch keine umfassenden Kenntnisse in diesem Bereich aufweisen können. Die entworfenen Versuche wurden in dieser Arbeit nachträglich didaktisch und methodisch aufgeschlüsselt. Dies und die einführenden Elemente stellen zusammen ein Nachschlagewerk dar, welches den Bearbeiter des entwickelten Praktikums beim Absolvieren unterstützen und den Einstieg in die Netzwerktechnik erleichtern soll. Ebenfalls Teil der vorliegenden Diplomarbeit waren die vollständigen Versuchsanleitungen, welche das Praktikum bilden[10].

Während der Anfertigung dieser Arbeit wurde das entwickelte Praktikum bereits zum ersten Mal an der Hochschule Mittweida (FH) durchgeführt. In anschließenden Befragungen war seitens der Studenten eine durchweg positive Resonanz zu verzeichnen. Fehler und Unklarheiten wurden während der Durchführung des Praktikums zur Kenntnis genommen und umgehend beseitigt. Bei den dieser Arbeit beiliegenden Versuchen handelt es sich um diese nachträglich verbesserten Versionen.

[10] Dieser Ausführung liegen die zum Zeitpunkt des Entstehens dieser Arbeit entwickelten Versuche. Die künftige Aktualisierung dieser liegt nahe. Die zum entsprechenden Zeitpunkt aktuellsten Versuchsversionen sind bei einem verantwortlichen Dozenten zu erhalten.

5.2 Ausblick

Die bisher entwickelten Versuche werden als Einführung in die Netzwerktechnik verstanden. Diese stellen jedoch in Bezug auf die verwendete Software Packet Tracer nur einen Teil der Möglichkeiten dieses Programms dar. Hier besteht die Aussicht auf Erweiterung des Praktikums durch weitere Teilversuche. Beispielsweise könnte mit Packet Tracer ein Szenario entworfen werden, in welchem bereits ein fertiggestelltes Netzwerk vorzufinden ist. Dieses wird mit falschen Konfigurationen ausgestattet, welche eine einwandfreie Funktion des Netzwerkes verhindern. Die Aufgabe der Studenten wäre das Erstellen einer Fehleranalyse und das Beseitigen von Unstimmigkeiten, um ein korrektes Arbeiten des Netzwerkes zu ermöglichen. Ebenfalls könnte der Umgang mit dem Cisco IOS-System weiter geschult werden, indem sich beispielsweise ein weiterer Versuch ausschließlich mit der Konfiguration eines Switches oder Routers per CLI beschäftigt.

Weiterhin bauen die entwickelten Versuche auf Packet Tracer in der Version 6.0.2 auf. Die zu diesem Zeitpunkt aktuelle Version 6.2 unterscheidet sich nur gering von der im Praktikum verwendeten und kann ebenfalls eingesetzt werden. Sollte jedoch eine neuere Version wichtige Funktionen einführen, welche den Gehalt der Versuche erhöhen könnte, ist an dieser Stelle eine Aktualisierung der Praktikumsanleitungen auf die verwendete Version möglicherweise angebracht. Dies gilt auch für Änderungen in der Handhabung, welche eventuell in neueren Versionen der Packet Tracer Software umgesetzt werden.

Literatur

[V01] Dipl.-Ing. (FH), M. Sc. Thomanek, Rico: Vorlesungsunterlagen: Netzwerktechnik und Administration I-III, Hochschule Mittweida, 2015

[V02] Prof. Dr.-Ing. habil. Winkler, Lutz: Vorlesungsunterlagen: Internet I – Aufbau, Adressierung, Betrieb, Hochschule Mittweida, 2014

[V03] Prof. Dr.-Ing. habil. Winkler, Lutz: Vorlesungsunterlagen: Internet II – Transportdienste und -protokolle, Hochschule Mittweida, 2013

[V04] Prof. Dr.-Ing. habil. Winkler, Lutz: Vorlesungsunterlagen: Internet III – Dienste und deren Anwendungsprotokolle, Hochschule Mittweida, 2014

[B01] Schnabel, Patrick: Computertechnik-Fibel: Grundlagen Computertechnik, Mikroprozessortechnik, Halbleiterspeicher, Schnittstellen und Peripherie, Books on Demand, 4. Auflage, 12/2015

[B02] Schnabel, Patrick: Netzwerktechnik-Fibel: Grundlagen, Übertragungstechnik und Protokolle, Anwendungen und Dienste, Sicherheit, Books on Demand, 3. Auflage, 06/2013

[B03] Schreiner, Rüdiger: Computernetzwerke: Von den Grundlagen zur Funktion und Anwendung, Carl Hanser Verlag GmbH & Co. KG, 5. Auflage, 05/2014

[Web01] Cisco System Trainingscenter

http://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html

[Web02] Cisco Networking Academy Packet Tracer

https://www.netacad.com/about-networking-academy/packet-tracer/

[Web03] Website von GNS-3

https://www.gns3.com/

[Web04] Boson NetSim

http://www.boson.com/netsim-cisco-network-simulator

[Web05] Cisco Systems IOS-Handbuch

http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r.html

[Web06] Elektronik Kopendium, Grundlagen Netzwerktechnik

http://www.elektronik-kompendium.de/sites/net/index.htm

[Web07] Seidel, Wolfram: Präsentation GNS-3, Hochschule Köln, 05/2012

http://www.it-bildungsnetz.de/fileadmin/media/Akademietag_2012/GNS3.pdf

Anlagen

Anlagen, Teil 1, Praktikumsanleitungen

Versuch 1: Packet Tracer – Einführung und Netzwerkgrundlagen

Studiengänge	▪ Medientechnik
Ausbildungsziel	▪ Kennenlernen der Packet Tracer Software ▪ Kennenlernen grundlegender Netzwerktechnologien
Ausbildungsinhalte	▪ Umgang mit der Packet Tracer Software ▪ Direkte Verknüpfung zweier Endgeräte ▪ Verknüpfung mehrerer Endgeräte via: • Hub • Switch ▪ Funktionsweisen von Hubs/Switches ▪ Visualisierung und Test von Datenübertragungen ▪ Einführung OSI-Referenzmodell
Hardware / Software	▪ 1 PC mit Virtual Box inklusive vorinstallierter Packet Tracer Software
Vorkenntnisse	▪ Theoretische Grundlagen der Vorlesungsunterlagen Netzwerktechnik und Administration I

Dieser Versuch soll zum einen eine Einführung in das Programm *Packet Tracer* und die Verwendung der programminternen Werkzeuge, zum anderen einen ersten grundlegenden Überblick über verschiedene Gebiete der Netzwerktechnik geben. Zu Beginn soll eine einfache Verbindung zweier handelsüblicher Rechner und eine Vernetzung mehrerer Geräte untereinander via Hub/Switch simuliert werden. Dabei soll zunächst auf die physikalische Verbindung der Geräte eingegangen und anschließend ein Ping zum Testen der erstellten Verbindung ausgeführt werden. Zugleich sollen Randinformationen zu den verschiedenen Technologien der Netzwerktechnik vermittelt werden. Für diesen und alle folgenden Versuche gilt es, ein abgeschlossenes Szenario über *File/ Save As …* zu speichern und anschließend per *File / New* ein neues Szenario zu öffnen.

Aufgabe 1: Vernetzung zweier handelsüblicher PCs

Zum Einsatz kommende Hardware:

2 Generic PCs (Standard PC)	
Copper Straight – Through (Standard Ethernet – Kupferkabel)	
Copper Cross – Over (Standard Crossover – Kupferkabel)	

Öffnen Sie das Programm Packet Tracer, welches sie unter *Start / Alle Programme / Cisco Packet Tracer* finden. Bei erstmaligem Starten der Software kann es zu folgendenden Fehlermeldungen kommen, welche jedoch bei der Durchführung des Praktikums keine Rolle spielen und somit ignoriert werden können (Abbildungen 1, 2, 3 und 4):

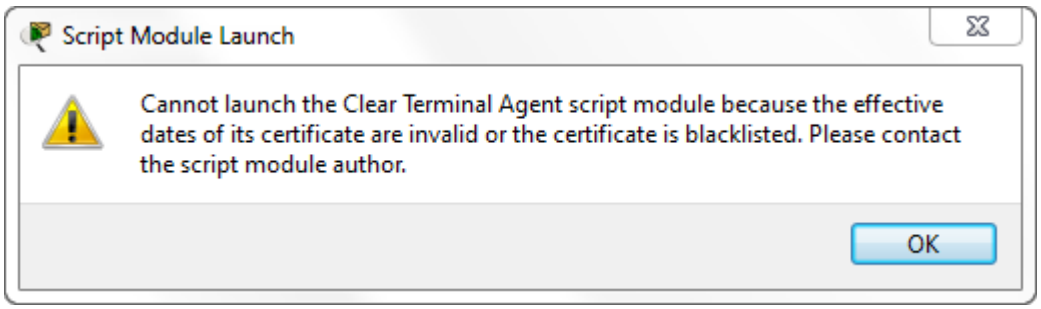

Abbildung 1

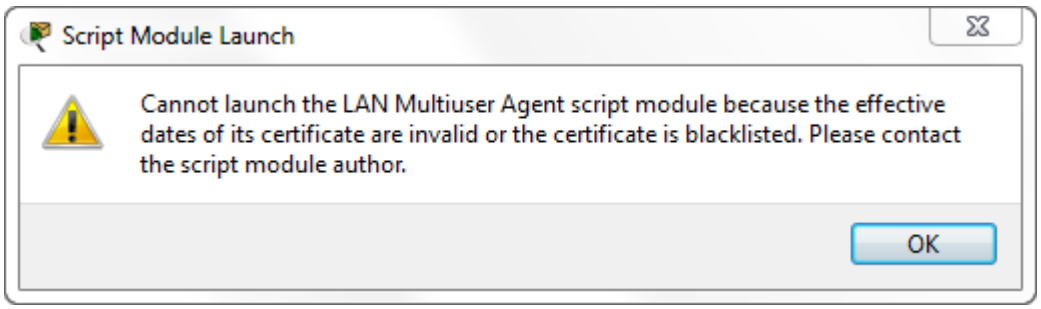

Abbildung 2

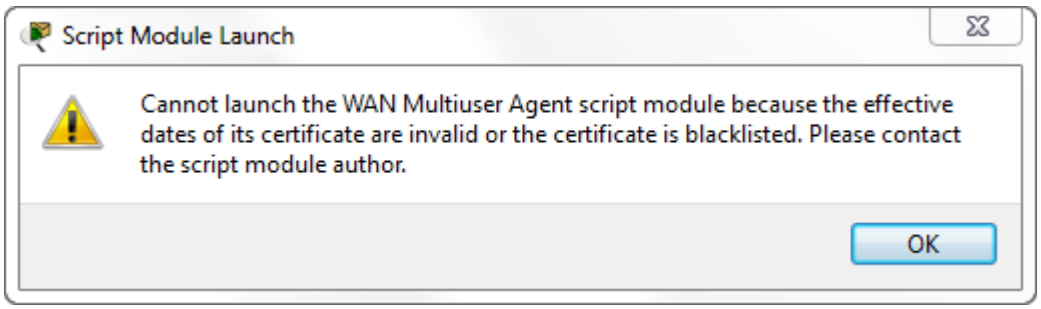

Abbildung 3

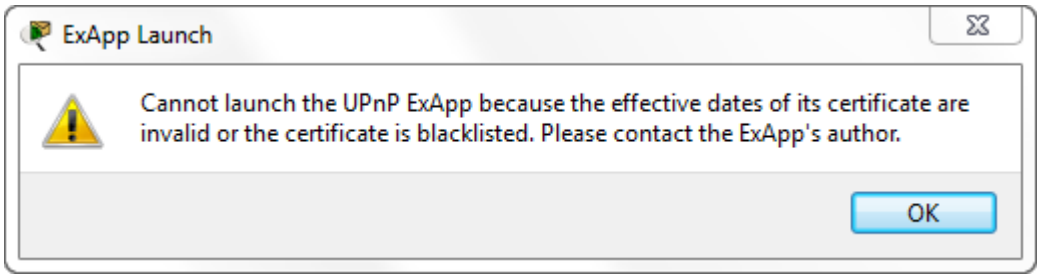

Abbildung 4

In einem ersten Schritt soll die Kommunikation zwischen zwei handelsüblichen PCs ermöglicht werden. Platzieren Sie daher zunächst die zwei Geräte auf der Arbeitsfläche. Begeben Sie sich hierfür in das Geräte – Manager Feld (Abbildung 5).

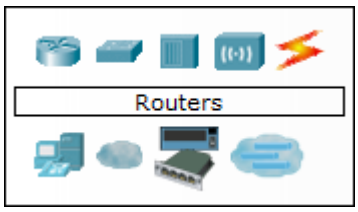

Abbildung 5

Hier klicken Sie auf  End Devices. Im nebenstehenden Untermenü sehen Sie eine Auflistung aller zur Verfügung stehenden Geräte. Klicken Sie auf den 

Generic-PC (PC-PT) und platzieren Sie ihn per weiterem Einfachklick an einer beliebigen Stelle des Arbeitsbereiches. Wiederholen Sie diesen Vorgang für einen weiteren Generic-PC.

Verbinden Sie nun die eben platzierten Geräte mit einem Standard-Kupferkabel. Dazu wählen Sie im Geräte Manager  *Connections*. Im erscheinenden Auswahlfeld klicken Sie auf  *Copper Straight-Through*. Zur Verbindung der zwei Computer klicken Sie zunächst auf den ersten PC und wählen *FastEthernet0* (Abbildung 6).

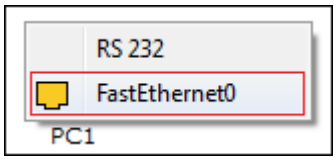

Abbildung 6

Das Kabel ist jetzt am FastEthernet-Port[1] des ersten PC angeschlossen. Ziehen Sie das Kabel jetzt zum zweiten PC und schließen Sie es per Einfachklick ebenfalls an dessen FastEthernet0-Port an. Wie Sie sehen, sind die Verbindungen rot gekennzeichnet (Abbildung 7).

[1] Unter Fast Ethernet wird in der Netzwerktechnik ein Übertragungsstandard verstanden. Dieser ist mit einer Übertragungsrate von 100 Megabit/s spezifiziert. Weitere Übertragungsraten reichen von 10 Megabit/s, über 1000 Megabit/s (*Gigabit-Ethernet*), bis hin zu 100 Gigabit/s (siehe auch Rubrik Übertragungsmedien – Kabeltypen, Vorlesungsskript Netzwerktechnik und Administration I).

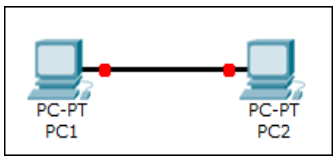

Abbildung 7

Da beide PCs mit einem Standard RJ45-Kabel verbunden sind, kann hier keine Kommunikation zwischen beiden stattfinden, da bei diesem Kabeltyp keine Kreuzung vorhanden und somit kein gleichzeitiges Senden *und* Empfangen möglich ist (siehe auch Rubrik Übertragungsmedien - Kabeltypen, Vorlesungsskript Netzwerktechnik und Administration I).

Entfernen Sie folgend das eben platzierte Kabel. Klicken Sie dazu auf das  *Delete-Symbol* in der Werkzeugpalette des Programms.

Anschließend bewegen Sie den Cursor über das Kabel und klicken Sie zum Entfernen auf dieses. Anstelle des eben entfernten Kabels setzen Sie nun ein *Crossoverkabel*. Wählen Sie dazu  *Copper Cross-Over* aus dem *Connections*-Menü und verbinden Sie beide Geräte so, wie bereits vorher beschrieben. Umgehend sind die Verbindungen grün gekennzeichnet, das heißt eine Kommunikation zwischen beiden Geräten ist jetzt prinzipiell möglich, da bei Crossover – Kabeln einer der beiden RJ45 Stecker gekreuzte Kabeladern aufweist und somit die direkte Verbindung zwischen zwei PCs ermöglicht. In der Praxis findet dies heutzutage jedoch keine Anwendung mehr, da praktisch alle modernen Netzwerkgeräte (Netzwerkkarten usw.) eine elektronische Kreuzung der Adern durchführen können, wenn benötigt.

Information: Packet Tracer speichert die jeweilige Werkzeugauswahl. Um weiter wie gewohnt auf der Arbeitsfläche agieren zu können, müssen Sie stets das  *Select* – Symbol aus der Werkzeugpalette wählen, beziehungsweise durch Betätigen der ESC-Taste auf der Tastatur in den entsprechenden Auswahlmodus zurückwechseln.

Als nächstes testen Sie die Kommunikationsfähigkeit der beiden Geräte untereinander. Es soll eine Paketübertragung mittels *Ping*[2] simuliert werden,

[2] Ping ist ein Diagnose-Tool zur Überprüfung der Erreichbarkeit eines Hosts innerhalb eines Netzwerkes.

welches die Pakete mittels *ICMP (Internet Control Message Protocol)*[3] überträgt. Damit sichergestellt ist, dass als Übertragung ausschließlich ICMP genutzt wird, müssen Sie dies zunächst einstellen. Wechseln Sie hierfür in den Simulationsmodus (Abbildung 8).

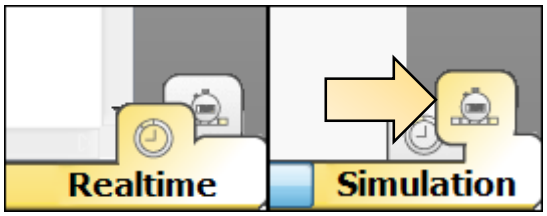

Abbildung 8

Der Simulationsmodus ermöglicht eine detaillierte Betrachtung von Paketübertragungen zwischen einzelnen Netzknoten. Weiterhin hat der Nutzer die Möglichkeit, zahlreiche, nach dem OSI – Referenzmodell kategorisierte Informationen einzusehen. Rufen Sie per Einfachklick auf *Edit Filters* die Liste mit allen verfügbaren Protokolltypen auf und lassen Sie nur *ICMP* aktiviert (Abbildung 9).

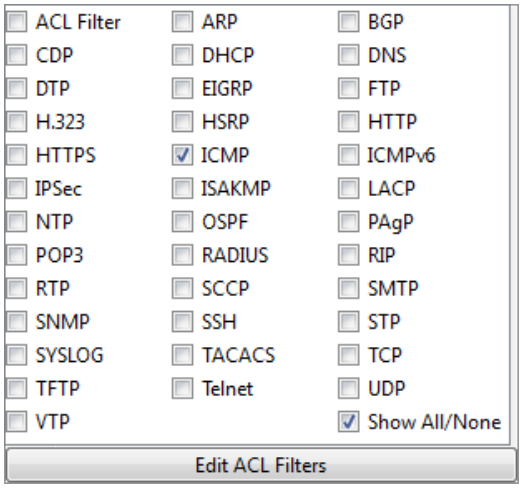

Abbildung 9

Nun wählen Sie eine einfache  *Protocol Data Unit (PDU)* aus der Werkzeugpalette. Eine Betätigung der Taste *P* hat den gleichen Effekt. Um jetzt eine Datenübertragung zu starten, klicken Sie zuerst auf den ersten PC und danach auf den zweiten. Die Fehlermeldung *PC1 has no functional ports* erscheint. Dies

[3] ICMP ist ein Protokoll, welches dem Informationsaustauschinnerhalb eines IPv4-Rechnernetzwerkes dient. Für IPv6-basierende Netzwerke existiert dazu das ähnliche *ICMPv6*.

liegt daran, dass noch keinem der beiden Geräte eine IP-Adresse zugewiesen wurde. Wechseln Sie zunächst zurück in den *Realtime Modus*.

Um dem ersten PC eine IP-Adresse zuzuweisen, führen Sie einen Einfachklick auf diesen aus. Das Konfigurationsfenster öffnet sich (Abbildung 10).

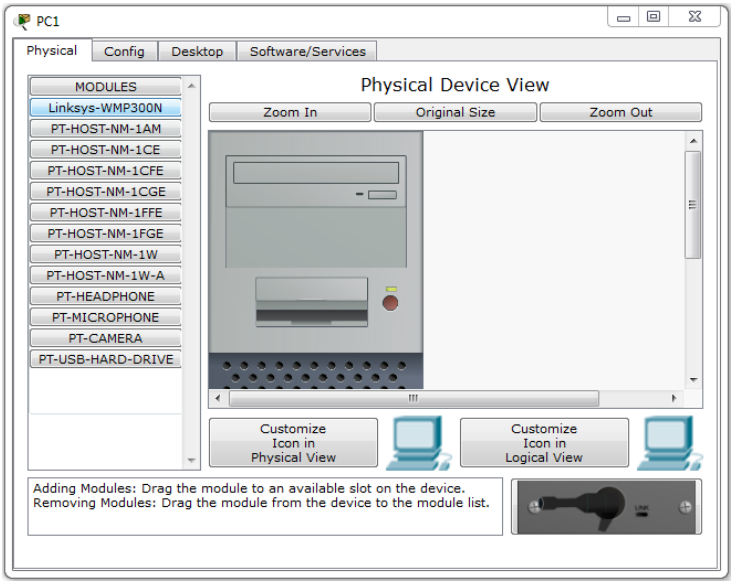

Abbildung 10

Auch hier kann bei erstmaligem Öffnen des Konfigurationsfensters ein Fehler auftreten (Abbildung 11).

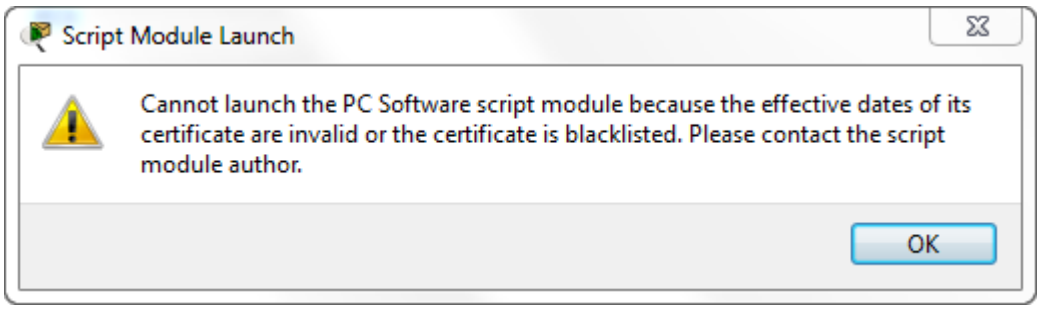

Abbildung 11

Auch hier handelt es sich um eine, für das Praktikum nicht relevante Meldung und kann ebenfalls außer Acht gelassen werden.

Wählen sie den Reiter *Desktop* (Abbildung 12).

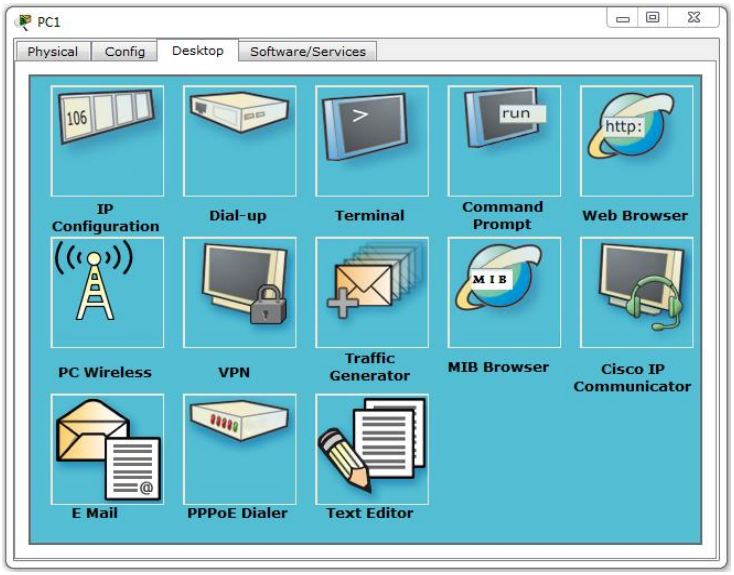

Abbildung 12

Öffnen Sie als nächstes die *IP Configuration* und wählen Sie mit *Static* die statische IP Zuweisung aus[4]. Tragen Sie jetzt in das Feld *IP Address* folgende IP Adresse ein: *192.168.0.1*

[4] In der Praxis erfolgt die IP-Vergabe automatisiert über DHCP (Dynamic Host Configuration Protocol). Dazu ist jedoch ein DHCP-Server erforderlich, welcher in diesem Versuch noch keine Anwendung findet.

Klicken Sie in das Feld *Subnet Mask*, wird automatisch die zugehörige Subnetzmaske eingesetzt, in diesem Fall *255.255.255.0* (Abbildung 13).

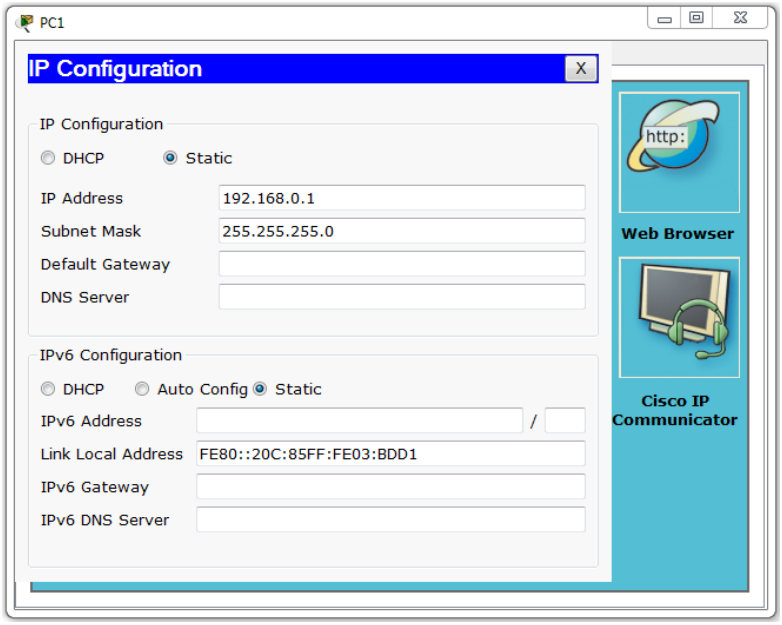

Abbildung 13

Die IP-Konfiguration ist damit abgeschlossen und Sie können das Fenster schließen. Wiederholen Sie diesen Vorgang für PC2 und setzen Sie die IP Adresse *192.168.0.2* ein. Jetzt sind beide Computer bereit, um miteinander zu kommunizieren.

Aufgabe 2: Visuelles Testen der Verbindung

Wählen Sie wieder eine einfache *Protocol Data Unit* aus der Werkzeugpalette und klicken Sie wieder zuerst auf den ersten, dann den zweiten PC. Diese Datenübertragung findet in Echtzeit statt und die Statusmeldung *Succesful* in der Eventliste verdeutlicht, dass sie auch erfolgreich war (Abbildung 14).

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)

Abbildung 14

Bedingt durch das Arbeiten von ARP[5] kann es vorkommen, dass der erste Übertragungsversuch fehlschlägt, da noch kein Eintrag im ARP – Cache vorhanden ist. In diesem Fall wiederholen Sie den Vorgang einfach. Stellen Sie deshalb vor jeder Übertragung im Simulationsmodus sicher, dass die Übertragung im Echtzeitmodus erfolgreich ist.

Um die eben stattgefundene Paketübermittlung zu visualisieren, wechseln Sie vom Echtzeitmodus in den Simulationsmodus. Klicken Sie im *Simulation Panel* unter *Play Controls* auf *Auto Capture / Play*. Jetzt können Sie den Weg des Datenpakets visuell verfolgen (Abbildung 15).

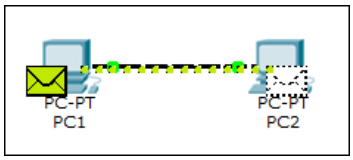

Abbildung 15

PC1 schickt das Datenpaket ordnungsgemäß an PC2. Nach Abschluss der Übertragung wird mit einem Briefsymbol verdeutlicht, ob die Übertragung  erfolgreich war oder  fehlgeschlagen ist.

Aufgabe 3: Testen der Verbindung über die Kommandozeile

In der Praxis ist dies die übliche Methode um herauszufinden, ob entsprechende Stationen über IP erreichbar sind. Rufen Sie das Konfigurationsfenster von PC1 per Einfachklick auf. Öffnen Sie erneut den Reiter *Desktop* und wählen Sie *Command Prompt*. Die Kommandozeile öffnet sich (Abbildung 16).

[5] ARP (Address Resolution Protocol) ist ein Protokoll zur Ermittlung der MAC – Adresse anhand der IP – Adresse (siehe auch Rubrik L2-Protokolle – ARP, Vorlesungsskript Netzwerktechnik und Administration II).

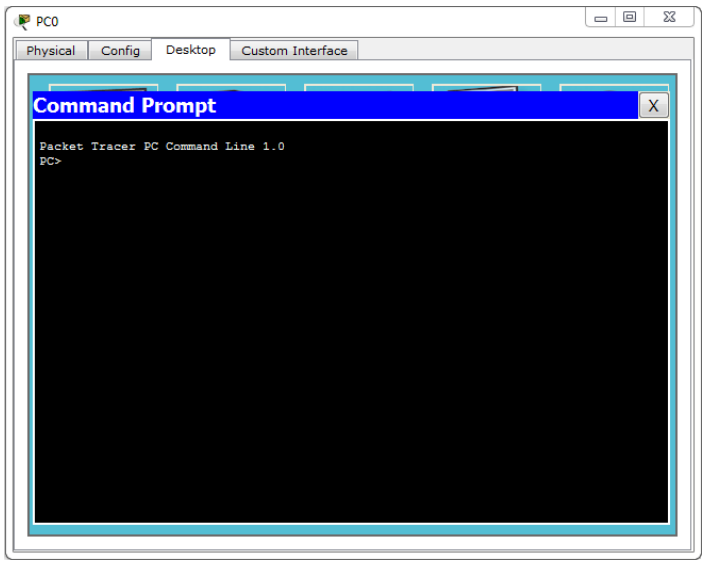

Abbildung 16

Um den vorher visualisierten *Ping* hier zu realisieren, geben Sie bitte Folgendes ein: *ping 192.168.0.2*
und schicken Sie den Befehl mit *Enter* ab. *Ping* sendet dadurch 4 ICMP-Pakete an PC2 mit der IP-Adresse 192.168.0.2. Nacheinander werden dessen Antworten in Verbindung mit der Paketgröße, der Übertragungszeit und der TTL (Time to live[6]) aufgelistet. Darunter wird zusätzlich eine Zusammenfassung über gesendete, empfange und verlorene Pakete, sowie die Durchschnittswerte der Übertragungszeiten abgebildet (Abbildung 17).

[6] Die TTL (Time to live) gibt die Gültigkeitsdauer von Daten in einem Netz an.

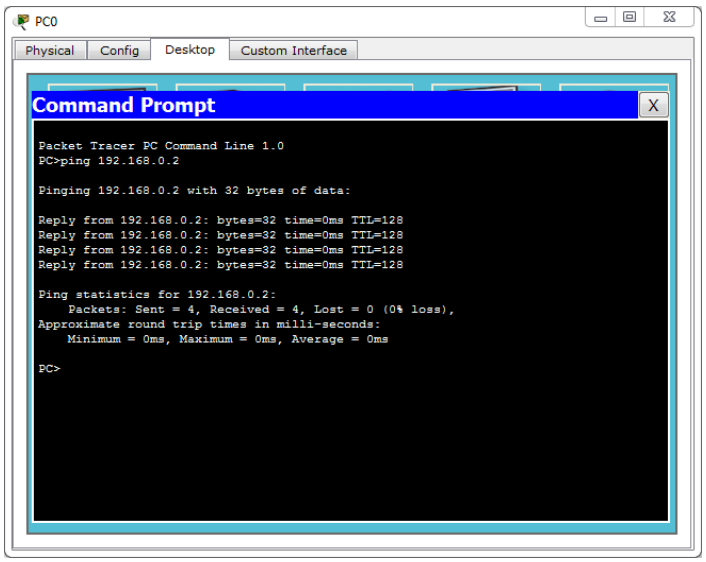

Abbildung 17

Aufgabe 4: Vernetzung mehrerer Geräte

Zum Einsatz kommende Hardware:

4 Generic PCs (Standard PC)

1 Generic Hub (Standard Hub)

1 2950 – 24 Switch (Standard 24 – Port Switch)

Im nächsten Schritt sollen mehrere Geräte miteinander vernetzt werden. Dies soll vorerst mit einem Hub realisiert werden. Richten Sie dazu zunächst ein Netzwerk mit 4 handelsüblichen PCs, welche über einen Hub verbunden sind, ein. Platzieren Sie dazu zunächst diese 4 Computer auf der Arbeitsfläche. Jetzt wählen Sie im Geräte Manager  *Hubs*. Verwenden Sie für dieses Beispiel einen  *Generic Hub (Hub-PT)*. Verbinden Sie anschließend alle PCs mit dem Hub. Benutzen Sie dafür ein geeignetes Kabel.

Weisen Sie jedem Rechner eine statische IP-Adresse zu. Um eine Konnektivität sicherzustellen, müssen sich diese im selben Netzwerk befinden[7]. Bei dem zu benutzenden Netzwerk soll es sich um ein Klasse C Netzwerk handeln. Ermitteln

[7] Kommunikation zwischen verschiedenen Netzwerken ist mit Hilfe von Routern möglich, was in diesem Versuch noch keine Anwendung findet.

Sie dazu geeignete IP Adressen, die dieses Kriterium erfüllen und weisen Sie diese den Geräten zu.

Schicken Sie jetzt eine PDU von einem PC zu einem anderen und wählen Sie als Übertragungsprotokoll ICMP. Hierbei ist es nicht relevant, um welche beiden PCs es sich handelt. Sollten Probleme auftreten, schauen Sie sich die genaue Vorgehensweise unter Aufgabe 1 noch einmal an. Verfolgen Sie nun per *Auto Capture / Play* im Simulationsmodus den Übertragungsweg der PDU und beobachten Sie dabei die Verhaltensweisen des Hubs. Da Hubs ausschließlich auf Schicht 1 (Bitübertragungsschicht) des OSI-Modells arbeiten und damit nicht in der Lage sind, Quelle oder Ziel des übertragenen Pakets zu identifizieren, werden diese zunächst an alle angeschlossenen Komponenten gesendet (Abbildung 18).

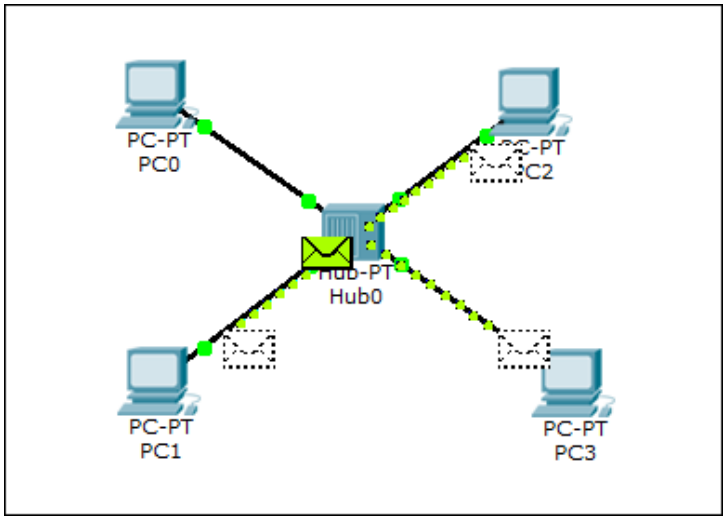

Abbildung 18

Im Endgerät wird dann mittels der Adressierungsinformationen überprüft, ob das Paket für dieses gesendet wurde. Im Falle einer Übereinstimmung wird eine Antwort vom Zielgerät an das Quellgerät zurückgeschickt. Diese Antwort wird vom Hub ebenfalls an alle Netzteilnehmer übertragen. Diesen Vorgang können Sie auch im Packet Tracer beobachten. Die Antwort erfolgt visuell äquivalent zum Senden. Nach Übertragungsabschluss erkennen Sie das Übertragungsergebnis wieder an dem Briefsymbol. In diesem Fall schlagen zwei Übertragungen fehl, während nur eines erfolgreich ist, da nur der PC antwortet, für den das Paket bestimmt ist (Abbildung 19).

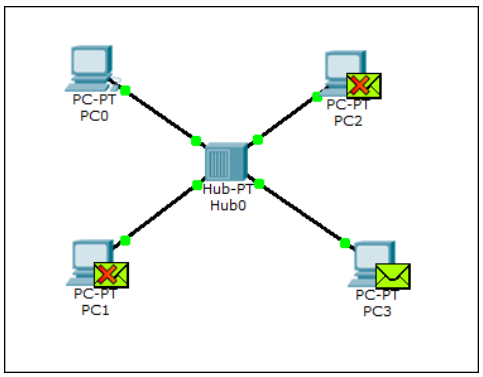

Abbildung 19

Per Einfachklick auf die einzelnen Briefsymbole können Sie weitere Informationen zum Übertragungsvorgang einsehen. Führen Sie einen Klick auf eines der fehlgeschlagenen Pakete aus. Packet Tracer zeigt anhand des OSI-Modells die einzelnen Schritte der Übertragung an. Wählen Sie Layer 2. Hier beschreibt Packet Tracer, dass die im Paket angegebene Ziel-Mac-Adresse nicht mit der Mac-Adresse des empfangenden Geräts übereinstimmt und das Paket dementsprechend verworfen wird (Abbildung 20).

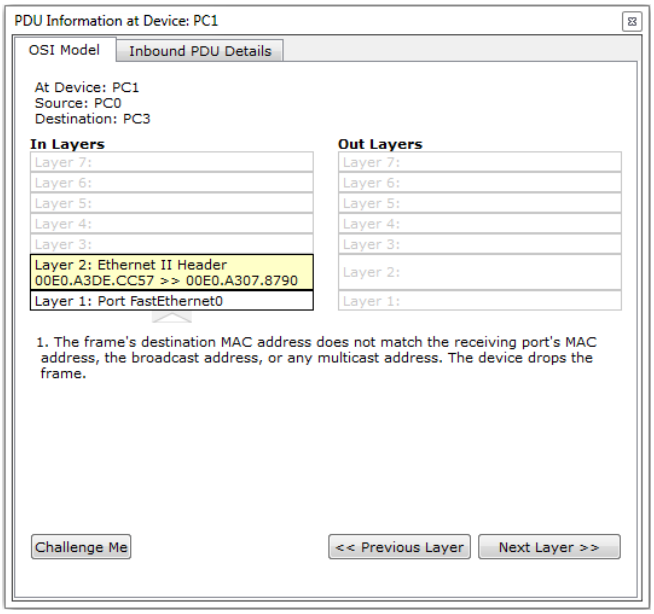

Abbildung 20

Hier wird die Funktionsweise von Hubs noch einmal verdeutlicht und zeigt auf, dass Hubs nicht dazu in der Lage sind, Daten gezielt an eine festgelegte Adresse zu übermitteln. Dadurch erhöht sich die Kollisionsdomäne des Netzwerks, was sich bei vielen Geräten auf die Übertragungsgeschwindigkeit auswirkt. Hubs wurden früher

aus Kostengründen eingesetzt und wurden deshalb nach der Senkung des Preisniveaus für Switches nahezu vollständig von diesen abgelöst. Um die Funktionsweise von Switches näher zu betrachten, tauschen Sie den platzierten Hub durch einen Switch aus. Wählen Sie hierzu Das Delete-Tool aus der Werkzeugpalette des Programms und entfernen die den Hub per Einfachklick auf diesen. Begeben Sie sich in das Geräte Manager Feld und wählen Sie *Switches*. Platzieren Sie einen 

2950-24-Switch anstelle des Hubs und verbinden Sie diesen mit den bereits vorhandenen 4 PCs. Um die unterschiedliche Funktionsweise von Hubs und Switches zu verdeutlichen, senden Sie erneut eine PDU von einem zu einem anderen PC und visualisieren Sie die Übertragung über *Auto Capture / Play*. Switches sind in der Lage, den Empfänger der zu übermittelnden Daten zu identifizieren. Dadurch wird das Paket nur an den dafür vorgesehenen Computer gesendet (Abbildung 21).

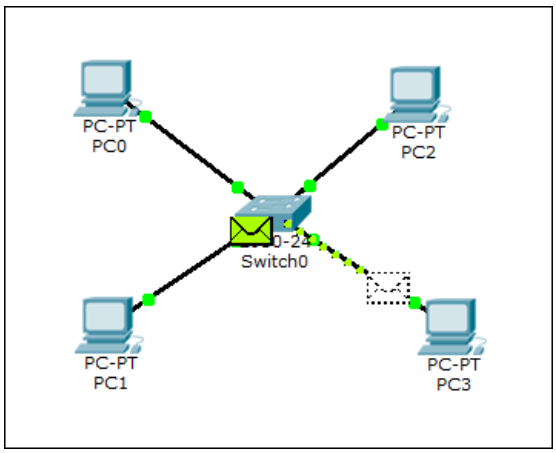

Abbildung 21

Aufgaben zum Versuch

1. Welche Kabelart ist für eine Direktverbindung zweier PCs geeignet und was macht diese besonders?

2. Nennen Sie die Unterschiede zwischen Hubs und Switches. Beziehen Sie sich dabei auch auf das OSI-Referenzmodell.

3. Was bedeutet ICMP?

4. Ermitteln Sie 4 IP Adressen, welche sich einem Klasse C Netzwerk zuordnen lassen. Nehmen Sie dazu die Vorlesungsunterlagen Netzwerktechnik und Administration II, Rubrik L3 – Adressierung.

Versuch 2: Packet Tracer – Weiterführung und Netzwerkgrundlagen

Studiengänge	▪ Medientechnik
Ausbildungsziel	▪ Kennenlernen weiterführender Netzwerktechnologien und Dienste ▪ Verstehen grundlegender Funktionsweisen von verschiedenen Technologien
Ausbildungsinhalte	▪ Einrichtung, Test und Betrachtung von: • DHCP – Server • DNS – Server • Mail – Server ▪ CSMA / CD ▪ Visualisierung der Paketübertragungswege ▪ Funktionsweisen von Hubs/Switches ▪ Verbindung zweier unterschiedlicher Netze
Hardware / Software	▪ 1 PC mit Virtual Box inklusive vorinstallierter Packet Tracer Software
Vorkenntnisse	▪ Versuch 1 ▪ Theoretische Grundlagen der Vorlesungsunterlagen Netzwerktechnik und Administration II

In diesem Versuch sollen die in Versuch 1 erworbenen Kenntnisse angewandt und weitergeführt werden. Inhalt dieses Versuches ist zum einen die Einrichtung einfacher DHCP-, DNS- und Mailserver, um die grundlegendenden Funktionsweisen dieser Technologien näher zu betrachten und zu verstehen. Zum anderen soll die in der Vorlesung betrachtete CSMA/CD – Technologie demonstriert werden. Weiterhin soll mit den bereits erworbenen Kenntnissen in der Netzwerktechnik und im Umgang mit der Software Packet Tracer ein einfaches Netzwerk simuliert werden, welches unterschiedliche Netze mit Hilfe von Routern miteinander verbindet. Dieser Versuch setzt den Abschluss des ersten Versuches voraus, grundlegende Schritte und bekannte theoretische Grundlagen werden in diesem Praktikum nicht mehr Schritt für Schritt erläutert.

Aufgabe 1: Einrichten eines DHCP – Servers

Zum Einsatz kommende Hardware:

3 Generic PCs (Standard PC)	
1 Generic Server (Standard Server, als DHCP – Server)	
1 2950 – 24 Switch (Standard 24 – Port Switch)	

In den vorangegangen Aufgaben wurden IP – Adressen stets statisch vergeben, was jedoch in der Praxis nur noch in Ausnahmefällen so gehandhabt wird. In den meisten Fällen wird dies von sogenannten DHCP[1] – Servern übernommen, welche die zu Verfügung stehenden IP – Adressen an die verschiedenen Clients vergeben. Um dies mit dem Packet Tracer zu realisieren, platzieren Sie zunächst die benötigten Geräte auf der Arbeitsfläche und verbinden Sie diese. Welche Geräte zum Einsatz kommen, entnehmen Sie wie gewohnt aus der Gerätetabelle, welche zu Beginn jeder Aufgabe zu finden ist. Anschließend verbinden Sie die PCs mit dem Switch und diesen wiederum mit dem Server, welcher später als DHCP – Server

[1] DHCP (Dynamic Host Configuration Protocol) ermöglicht die automatische Zuweisung von Netzwerkkonfigurationen an einen Clienten durch einen Server.

fungieren soll. Das soeben erstellte Netzwerk sollte in etwa wie folgt aussehen (Abbildung 1):

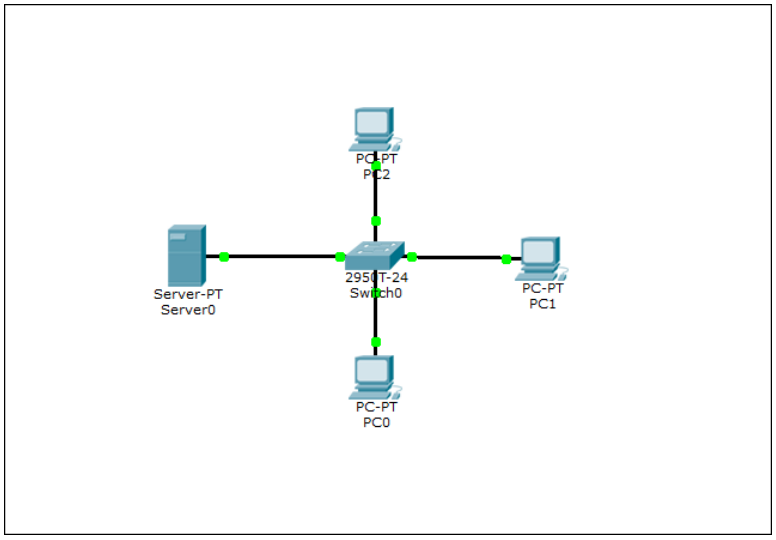

Abbildung 1

Begeben Sie sich in die IP Konfiguration des ersten PCs und wählen Sie als Zuweisungsmethode *DHCP* aus (Abbildung 2).

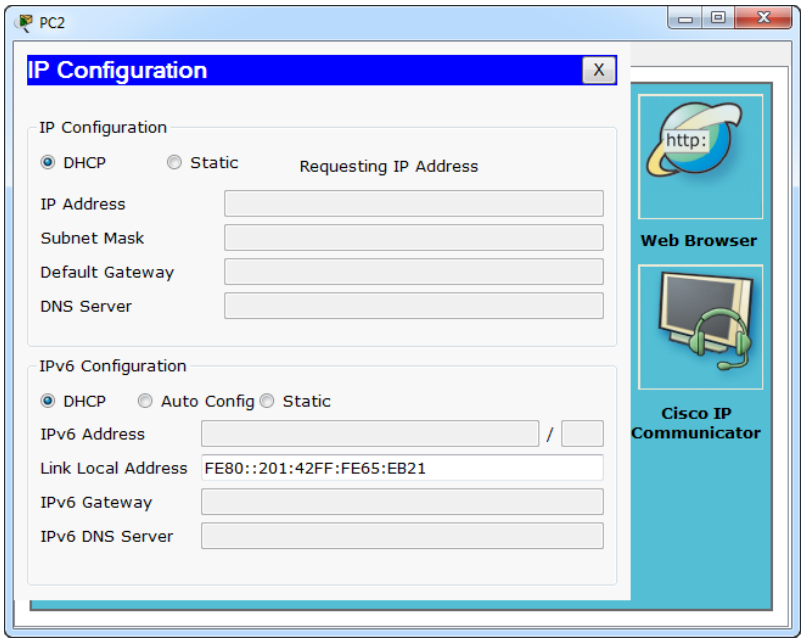

Abbildung 2

Anhand der Meldung *Requesting IP Address* erkennen Sie, dass eine passende Netzwerkkonfiguration angefordert wird. Diese Anforderung wird zum jetzigen Zeitpunkt jedoch erfolglos bleiben, da der DHCP – Server noch nicht ordnungsgemäß konfiguriert ist und demnach keine Funktion aufweist. Öffnen Sie

jetzt per Einfachklick auf den 

Generic – Server (Server – PT) und wählen Sie *Config* (Abbildung 3).

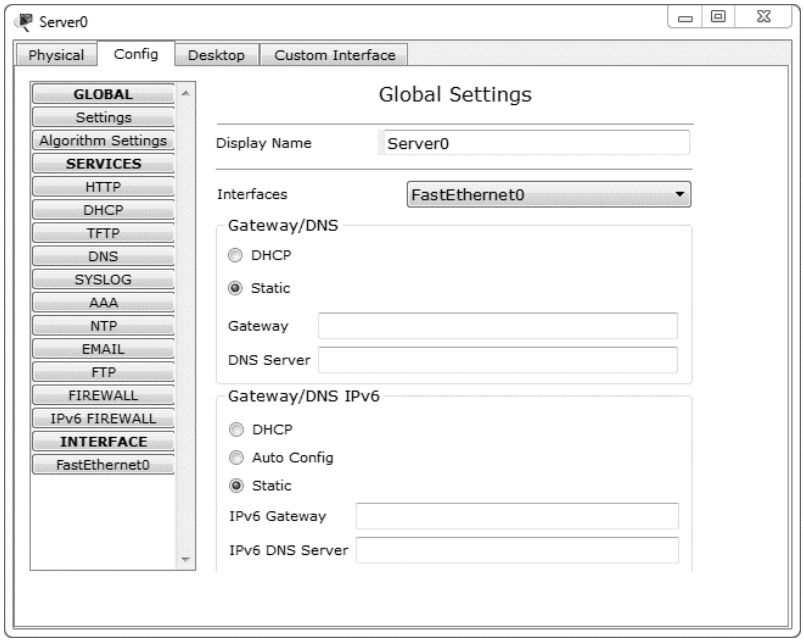

Abbildung 3

Hier sehen Sie sämtliche Konfigurationsmöglichkeiten des Servers. Diese Aufgabe konzentriert sich vorerst auf die dynamische Zuweisung von Netzwerkkonfigurationen. Rufen Sie also den Menüpunkt *DHCP* auf (Abbildung 4).

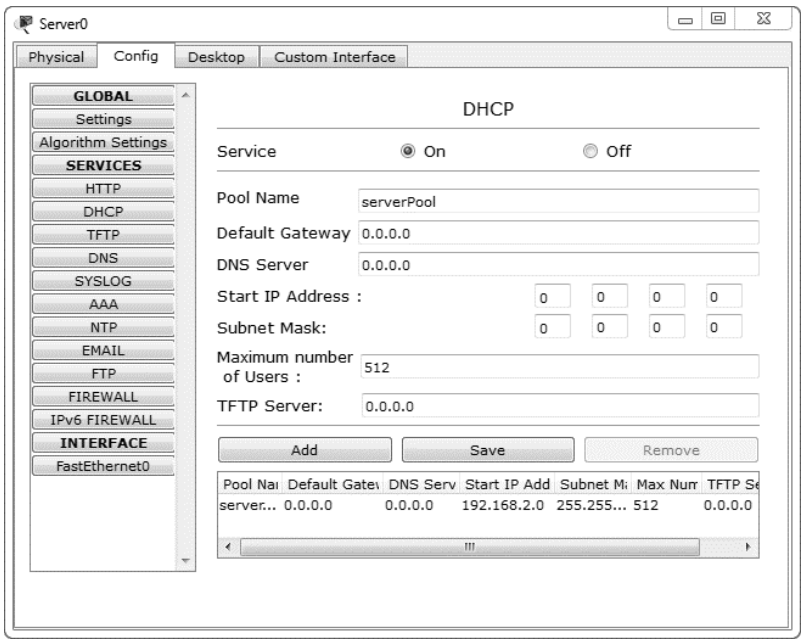

Abbildung 4

Unter diesem Punkt können Sie die zu verteilenden Netzwerkparameter (wie IP – Adressenbereich, Standard Gateway usw.) konfigurieren. Um die Funktionsweise zu demonstrieren, tragen im Feld *Start IP Adress* eine gewünschte IP Adresse und unter *Subnet Mask* eine dazu passende Subnetzmaske ein. Anschließend bestätigen Sie ihre Einstellung mit einem Einfachklick auf *Save* und vergewissern Sie sich, dass der Service aktiviert ist (Checkbox Service *On*). Da der Server in diesem Beispiel zu Testzwecken lediglich über einen Switch mit den Endgeräten verbunden ist, wird hier keine Angabe zu *Default Gateway* benötigt. Jedoch muss sichergestellt werden, dass sich der Server im gleichen Netz mit den angeschlossenen Geräten befindet, um eine einwandfreie Funktion zu gewährleisten. Öffnen Sie hierzu das Feld *FastEthernet0* (Abbildung 5).

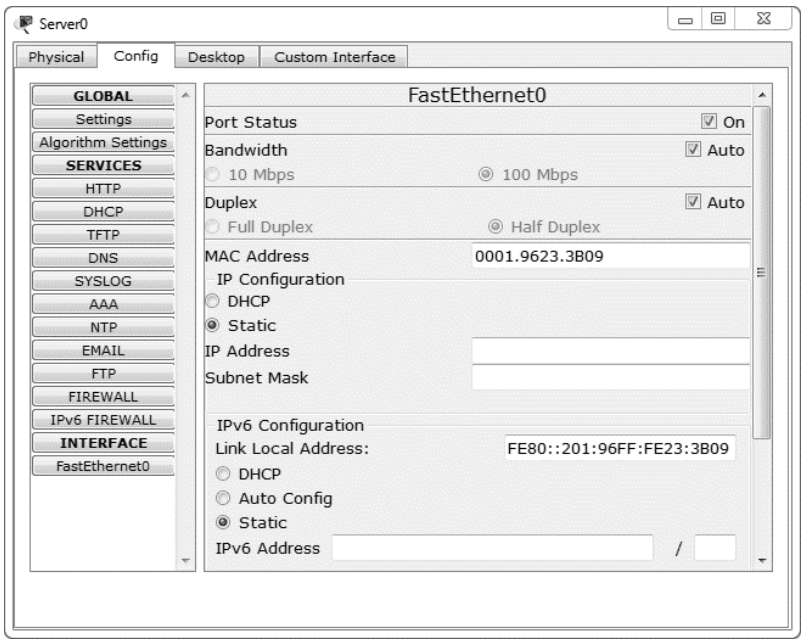

Abbildung 5

Unter *IP Configuration* tragen Sie eine, zu dem von Ihnen gewählten IP – Bereich passende IP – Adresse, sowie Subnetzmaske in die dafür vorgesehenen Felder ein. Die Konfiguration im Server ist jetzt abgeschlossen. Schließen Sie das Fenster. Begeben Sie sich nacheinander in die IP – Konfigurationsfenster der PCs und wählen Sie unter IP – Configuration DHCP. Die Rechner bekommen nun vom Server die vorher konfigurierte IP – Konfiguration zugewiesen (Abbildung 6).

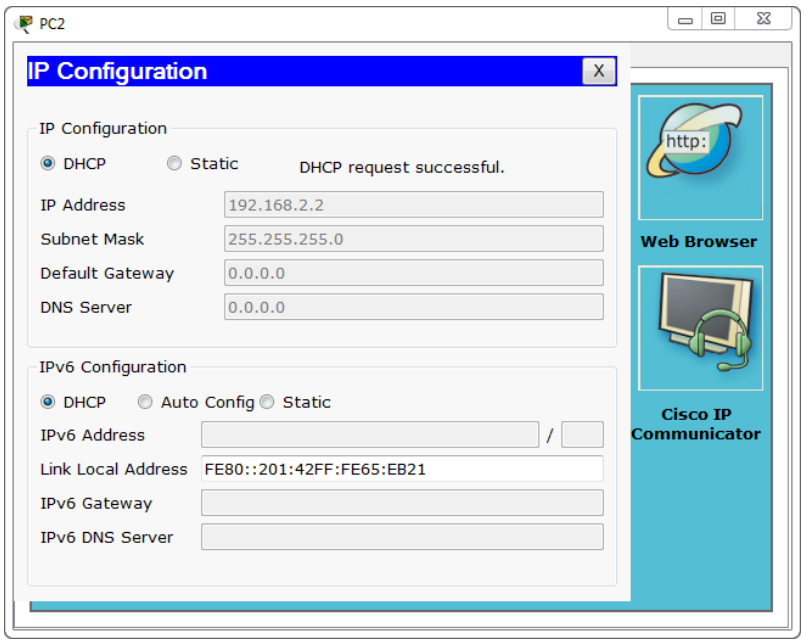

Abbildung 6

Um die Schritte zwischen Client und DHPC – Server zu analysieren, die letztlich zu einer IP – Zuweisung führen, begeben Sie sich in den Simulationsmodus. Wählen Sie in der Event Filter Liste *DHCP* aus. Zurück in der IP – Konfiguration eines PCs schalten Sie zunächst auf Static und anschließend wieder auf DHCP, um einen DHCP – Anforderung zu initiieren. Anhand der beiden Briefsymbole, welche am PC erscheinen, erkennen Sie, dass der Request beginnt. Bei dem ersten Paket (links) handelt es sich um ein DHCP – Release[2]. Dies soll hier jedoch nicht beachtet werden. Führen Sie einen Einfachklick auf das zweite Paket aus und werfen Sie einen Blick auf *Layer 7* der *Out Layers* (Abbildung 7).

[2] Ein DHCP – Release gibt die eigenen Einstellungen wieder frei, um sie für andere Clients im Netz verfügbar zu machen. Dies tritt beispielsweise ein, wenn die IP vor Ende der Lease Zeit zurückgegeben werden soll.

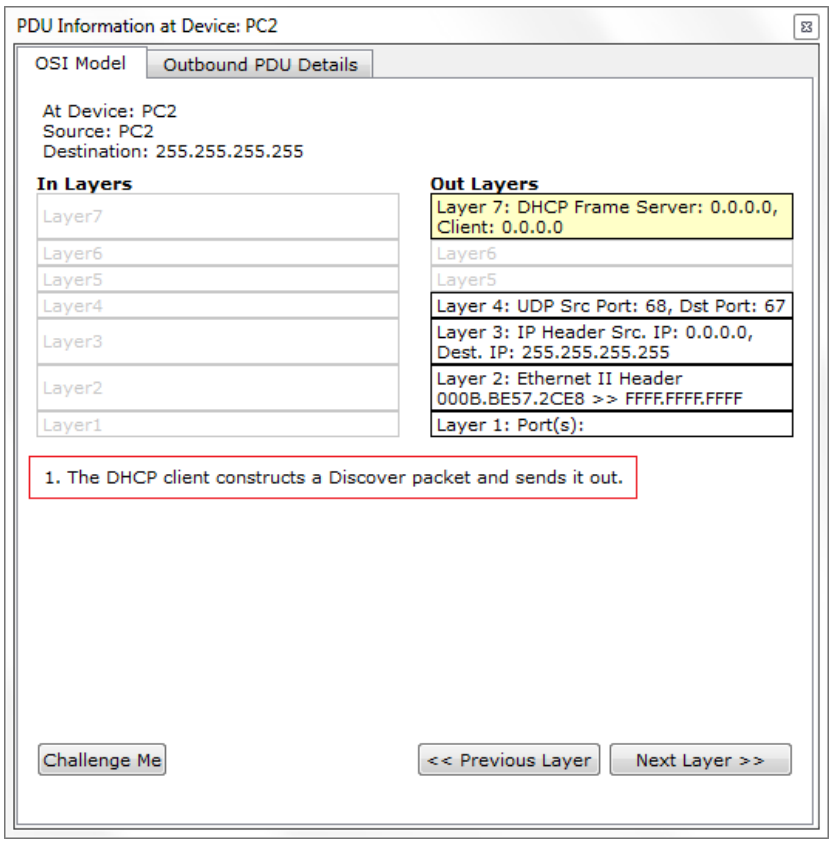

Abbildung 7

Es wird nun ein *Discover packet*[3] gesendet. Schließen Sie die Detailansicht und verfolgen Sie mittels *Capture / Forward* die Paketübertragung bis zum Server. Achten Sie darauf, dass Sie die Übertragung so vorantreiben, bis das *zweite* Paket am Server angekommen ist. Öffnen Sie erneut das Detailfenster der Übertragung und betrachten Sie *Layer 7* der *In Layers* (Abbildung 8).

[3] Der Client sendet eine Broadcast – Anfrage an alle, sich im selben Netz befindliche Server und frag Adressangebote ab.

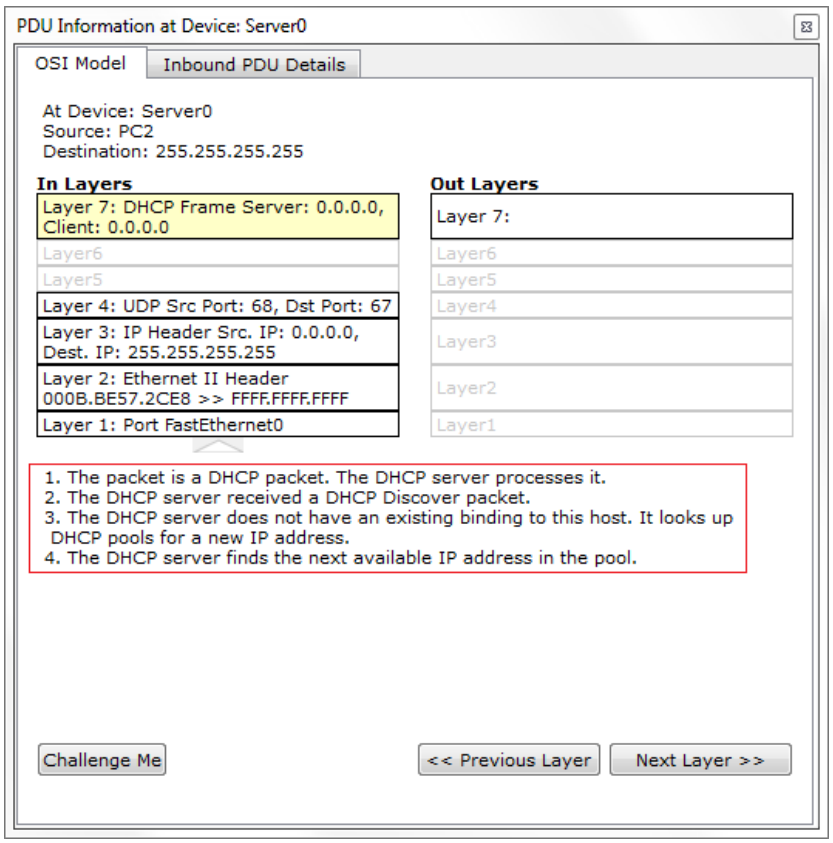

Abbildung 8

Der DHCP – Server erkennt das *Discover packet* und sucht nach verfügbaren IP – Adressen im festgelegten Pool. Der Server findet eine verfügbare IP – Adresse. Schalten Sie auf *Layer 7* der *Out Layers* um (Abbildung 9).

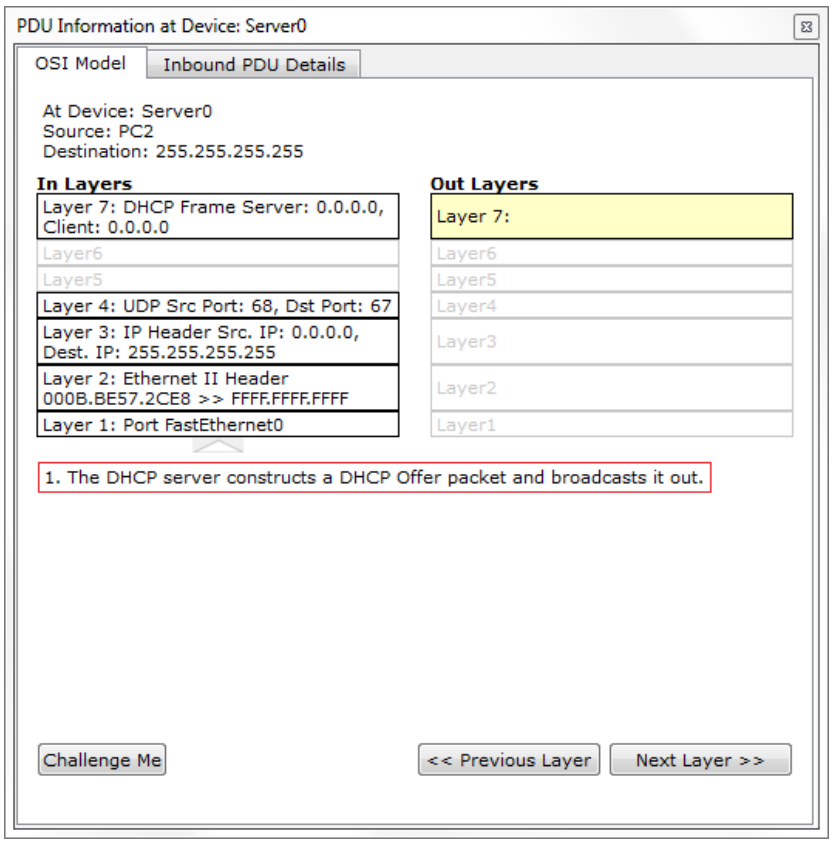

Abbildung 9

Der DHCP – Server erstellt basierend auf dem *Discover packet* folglich ein *Offer packet* und sendet dieses als Broadcast ab. Schließen Sie das Fenster und verfolgen Sie das Paket weiter, bis es wieder beim PC eintrifft. Führen Sie erneut einen Einfachklick auf das Briefsymbol aus und betrachten Sie wieder *Layer 7* der *In* und *Out Layers* (Abbildung 10 und 11).

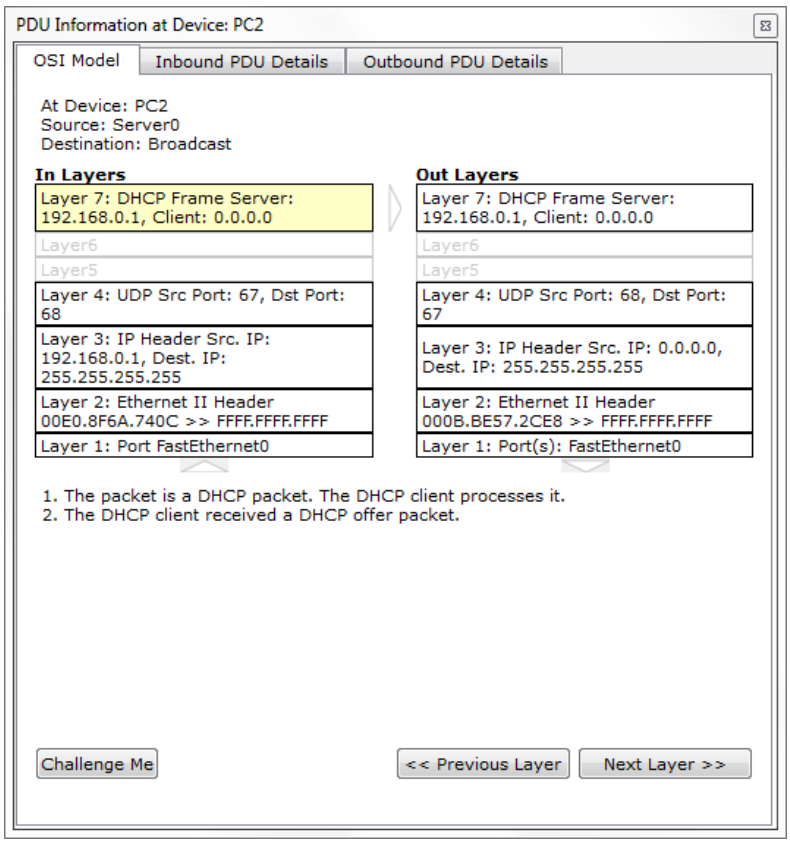

Abbildung 10

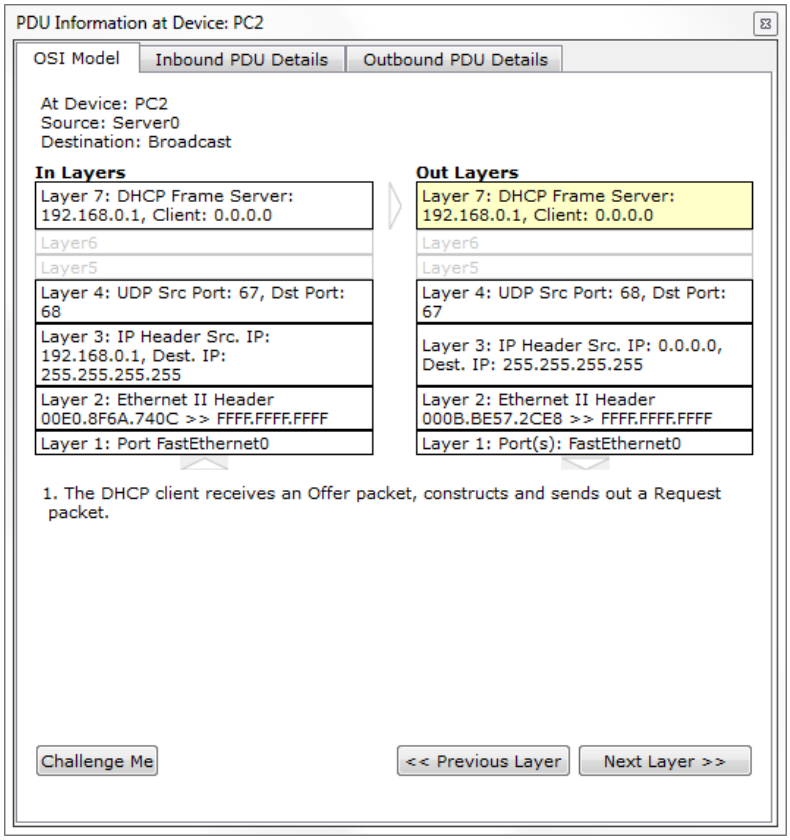

Abbildung 11

Der Client erhält und erkennt das *Offer packet* und erstellt dementsprechend ein *Request packet* (Anfrage an den Server, die ausgesuchte IP – Adresse zu erhalten). Verfolgen Sie die Übertragung zurück zum Server, öffnen Sie erneut die Paketinformationen und betrachten Sie *Layer 7* der *In Layers* (Abbildung 12).

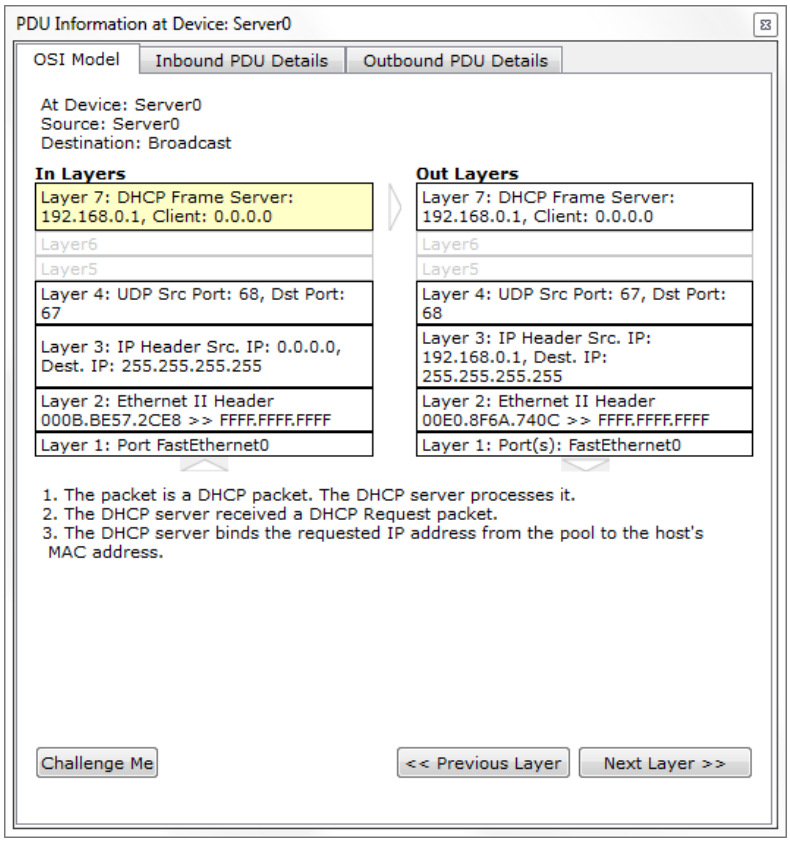

Abbildung 12

Der Server erhält die vom Client gesendete Anfrage und bindet die ausgewählte IP – Adresse an die MAC – Adresse des Client. Diese Informationen werden in einem weiteren Paket zurück an den Client gesendet, dort verarbeitet und in dessen IP – Konfiguration eingetragen (Abbildung 13).

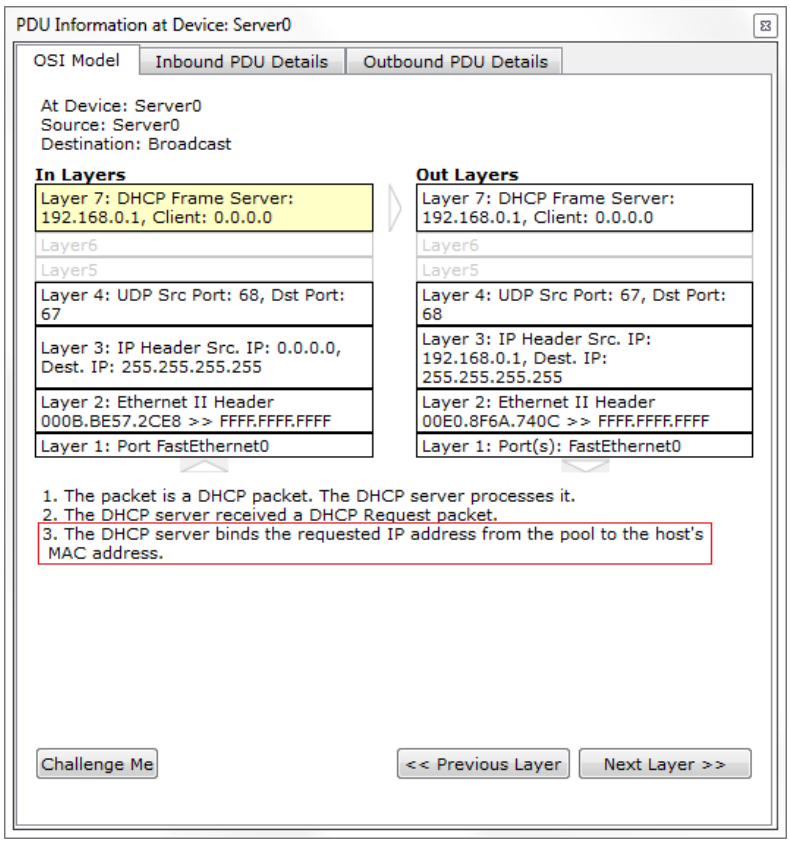

Abbildung 13

Durch die vollständige Konfiguration können die Geräte untereinander kommunizieren, ohne dass vorher die Netzwerkparameter statisch vergeben werden mussten. Fügt man jetzt weitere Geräte zum Netzwerk hinzu, werden diese ebenfalls dynamisch in das Netzwerk eingebunden, sobald DHCP bei diesen aktiviert wird. Begeben Sie sich zurück in den Echtzeitmodus und testen Sie die Konnektivität zwischen den Geräten mittels einer *Protocol Data Unit (ICMP)* oder per *Ping* über die Kommandozeile.

Aufgabe 2: Einrichten eines DNS – Servers

Zum Einsatz kommende Hardware:

3 Generic PCs (Standard PC)

3 Generic Server (Standard Server, als DNS – Server)

1 2950 – 24 Switch (Standard 24 – Port Switch)

DNS[4] ist ein wichtiger Dienst, um beispielsweise eine einfach zu merkende Webadresse in die zugehörige IP umzuwandeln und umgekehrt. Dieser Dienst soll jetzt mit dem Packet Tracer simuliert werden, um Ihnen einen Überblick über die grundlegende Funktionsweise von DNS zu verschaffen. Zu Beginn wird ein überschaubares Netzwerk aus 3 PCs, einem Switch und 3 Servern aufgebaut. Dies sollte in etwa wie folgt aussehen (Abbildung 14):

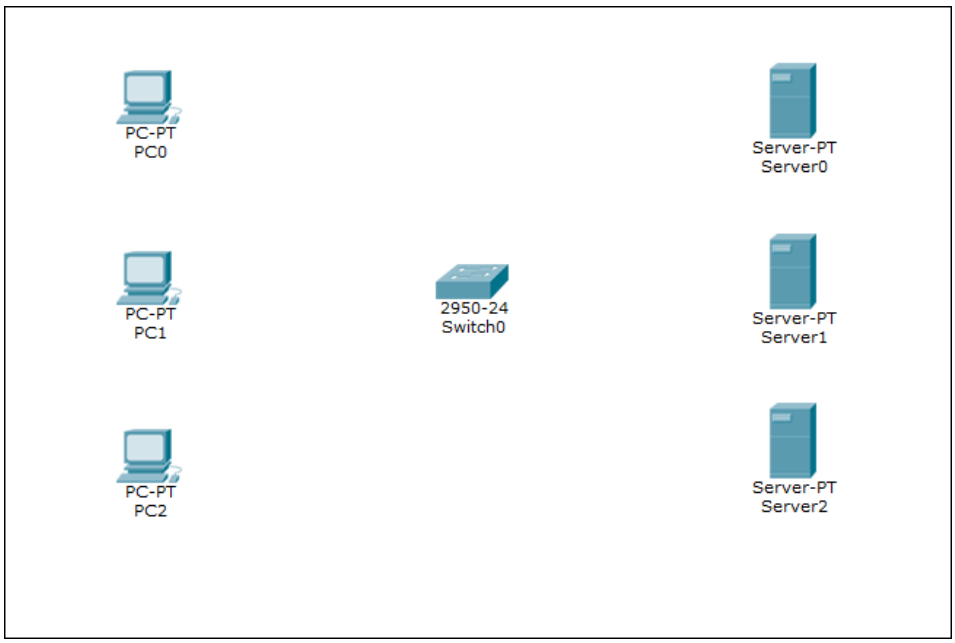

Abbildung 14

In diesem Szenario soll *Server0* als *DHCP – Server* fungieren. Richten Sie diesen entsprechend ein. Sollte es zu Problemen kommen, nehmen Sie sich Aufgabe 1 zur Hilfe. Binden Sie die 3 Computer und die 3 Server an den Switch an. Aktivieren Sie die DHCP – Zuweisung auf den PCs und prüfen Sie, ob diese die von Ihnen konfigurierten Einstellungen erhalten. Wenden Sie sich *Server1* zu, welcher als DNS – Server dienen soll. Dieser enthält eine Übersetzungstabelle, in welcher sämtliche IP – Adressen und die dazugehörigen Namen gespeichert sind, um diese später bei Anfragen durch einen Client entsprechend zuordnen zu können. Im Moment existieren jedoch noch keine Einträge, welche Sie in diese Tabelle eintragen könnten. Hier kommt *Server2* ins Spiel. Als Beispiel definieren wir als

[4] DNS (Domain Name System) ist ein Dienst zur Namensauflösung in IP – basierten Netzwerken. Es dient der Umwandlung und Zuordnung einer IP – Adresse in einen, für den Menschen einfacher merkbaren Namen.

Namen *www.hs-mittweida.de*. Dies soll den Webserver der Hochschule Mittweida repräsentieren. Öffnen Sie per Einfachklick auf Server2 dessen Konfigurationsoberfläche und begeben Sie sich über den Reiter Desktop in dessen Desktop – Umgebung (Abbildung 15).

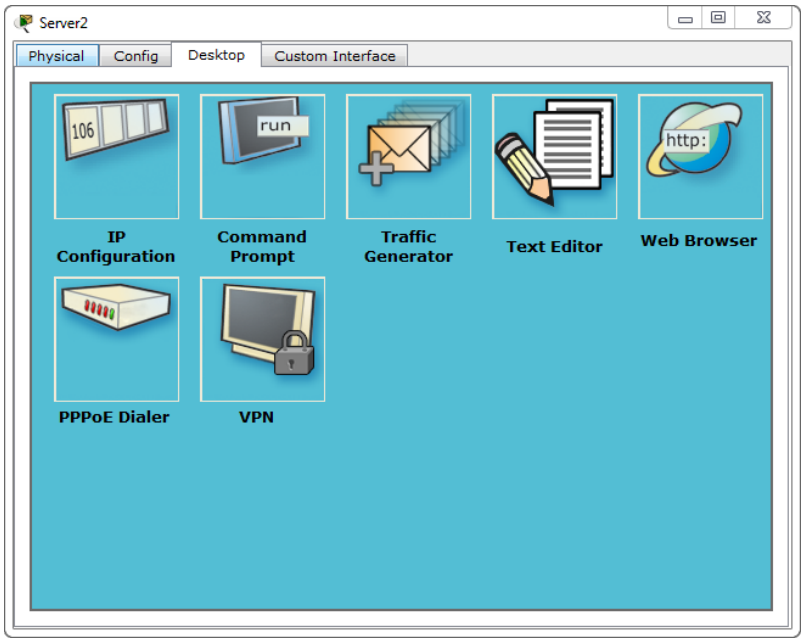

Abbildung 15

Wählen Sie IP Configuration und vergeben Sie IP – Adresse und Subnetzmaske passend zu Ihrer DHCP – Konfiguration (diese IP – Adresse wird später in die Namenstabelle des DNS – Servers eingetragen). Um das Endergebnis visuell ansprechender zu gestalten, begeben Sie sich jetzt in den *Config* – Tab, wählen Sie den Punkt *HTTP*[5] und ersetzen sie den schon vorhandenen HTML – Code mit Folgendem (Abbildung 16):

[5] HTTP (Hypertext Transfer Protocol) ist ein Kommunikationsprotokoll im World Wide Web. Es wird hauptsächlich dazu genutzt, um auf Hypertext basierende Dokumente (Webseiten) vom Server anzufordern und diese zur Darstellung in Webbrowser zu laden. Darüber hinaus kann es auch als allgemeines Datenübertragungsprotokoll genutzt werden.

<html>

* Hochschule Mittweida - University Of Applied Sciences *

<hr>Herzlich Willkommen an der Hochschule Mittweida

* Weiterführende Links:*

* *

*
Fakultät Medien*

* *

*
Fakultät Ingenieurswissenschaften*

* *

*
Soziale Arbeit*

</html>

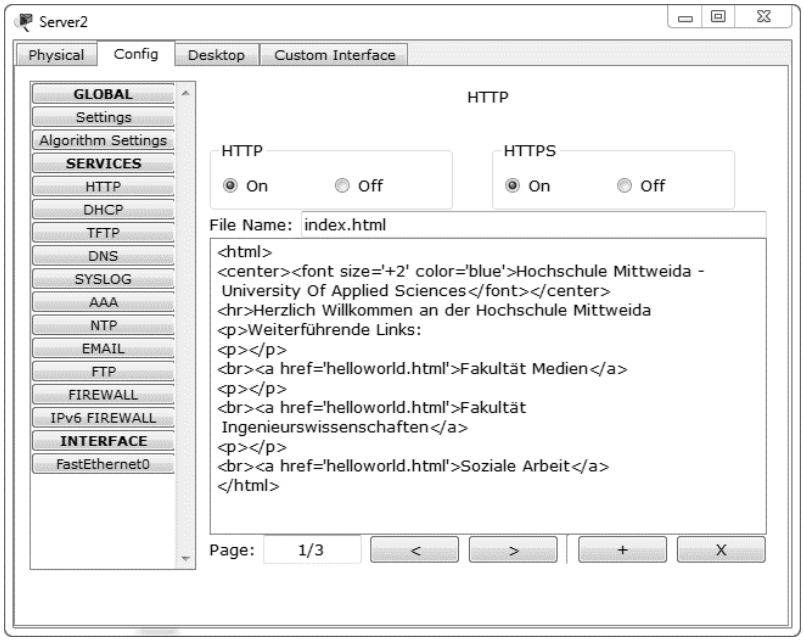

Abbildung 16

Die Konfiguration von Server2 ist damit abgeschlossen. Sie können das Konfigurationsfenster schließen. Öffnen Sie anschließend die Konfigurationsoberfläche eines beliebigen PCs, navigieren Sie zu dessen Desktopoberfläche und öffnen Sie den *Web Browser* (Abbildung 17).

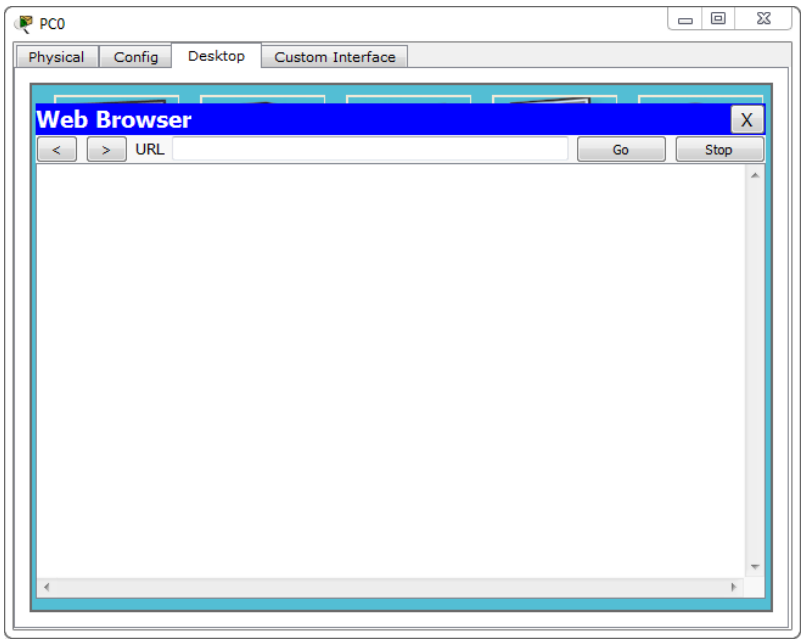

Abbildung 17

Geben Sie den vorher festgelegten Namen für Ihre Webseite *www.hs-mittweida.de* in die Adresszeile ein und bestätigen Sie mit Enter. Wie Sie sehen, bleibt das Fenster leer (Abbildung 18).

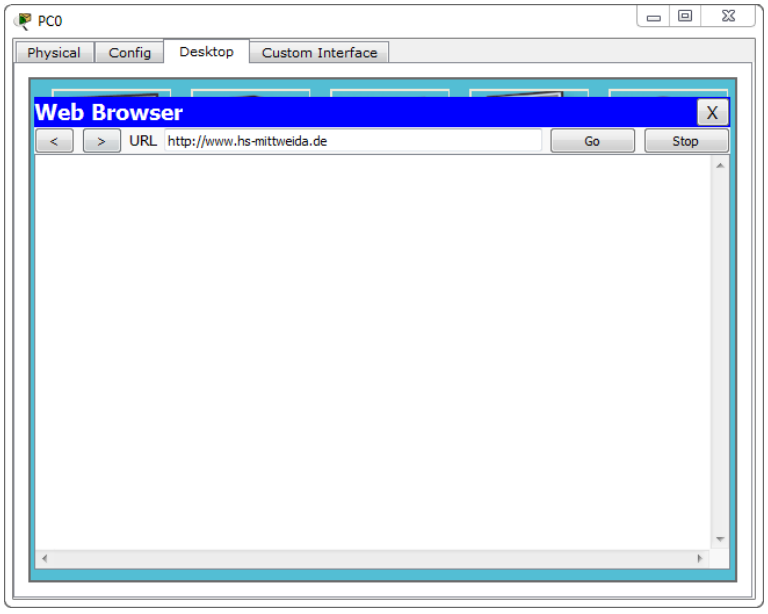

Abbildung 18

Dies liegt daran, dass das Netzwerk noch nicht mit dem Namen *www.hs-mittweida.de* umgehen kann, da der Eintrag in der Tabelle des DNS – Servers noch nicht vorhanden und dieser den Clients noch nicht bekannt ist. Um den DNS – Server zu konfigurieren, begeben Sie sich zurück in das Konfigurationsfenster von

Server1. Vergeben Sie im Untermenü *IP Configuration* unter dem Reiter *Desktop* eine zum Netz passende IP Konfiguration. Diese IP muss später dem DHCP – Dienst noch hinzugefügt werden, um sie automatisch an die Clients zu übermitteln. Rufen Sie anschließend den Reiter *Config* auf. Über die Schaltfläche DNS gelangen Sie in jenes Menü, in dem Sie die benötigten Einstellungen vornehmen können. Tragen Sie hier bei *Name* www.hs-mittweida.de und bei *Address* die an Server2 zugewiesene IP – Adresse ein (Abbildung 19).

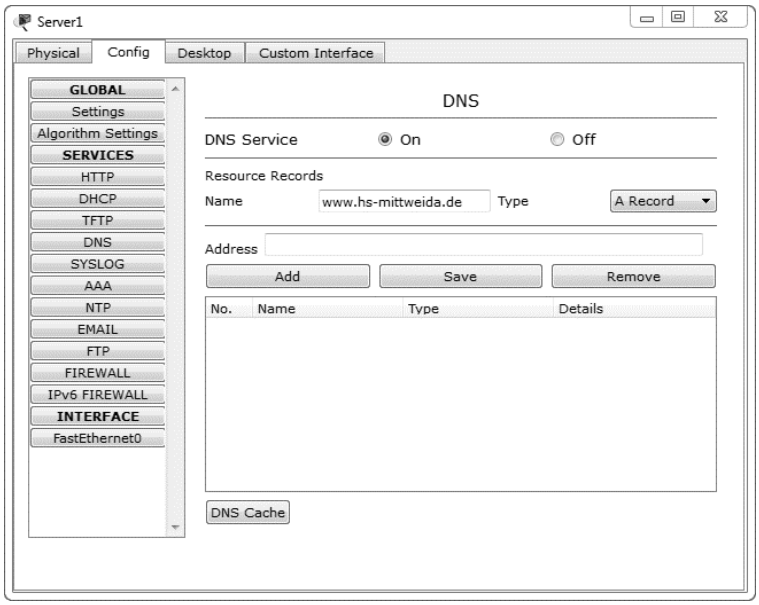

Abbildung 19

Über die Schaltfläche *Add* fügen Sie den eben erstellten Eintrag hinzu. Der DNS – Server kennt den Zusammenhang zwischen Adresse und IP – Adresse und kann diese jeweils untereinander auflösen. Stellen Sie den DNS – Service von *Off* auf *On* und schließen Sie das Fenster. Weiterführend fügen Sie die für *Server1* festgelegte IP Adresse dem DHCP – Dienst von *Server0* hinzu. Öffnen Sie dazu die Oberfläche von *Server0* und navigieren Sie über *Config* ins Untermenü *DHCP*. Wählen Sie Ihren Eintrag per Einfachklick aus und ändern Sie die IP Adresse im Feld *DNS Server* in die IP Adresse von *Server1*. Damit die Clients diese Einstellungen übernehmen, öffnen Sie deren IP Konfiguration und schalten Sie von *DHCP* auf *Static* und zurück, um die Einstellungen zu aktualisieren.

Um den DNS Service zu testen, öffnen Sie erneut den Webbrowser eines PCs und geben Sie als Adresse noch einmal *www.hs-mittweida.de* ein und schicken sie den Request ab. Der Name wird durch den DNS – Server in die zugehörige IP – Adresse

umgewandelt, damit der *Request* dem jeweiligen Webserver zugeordnet werden kann. Hier fordert dieser jetzt das entsprechende Dokument (in diesem Fall die vorher erstellte HTML – Seite), welches per *Response* an den anfragenden Client (hier der Webbrowser) zurückgesendet und dargestellt wird (Abbildung 20).

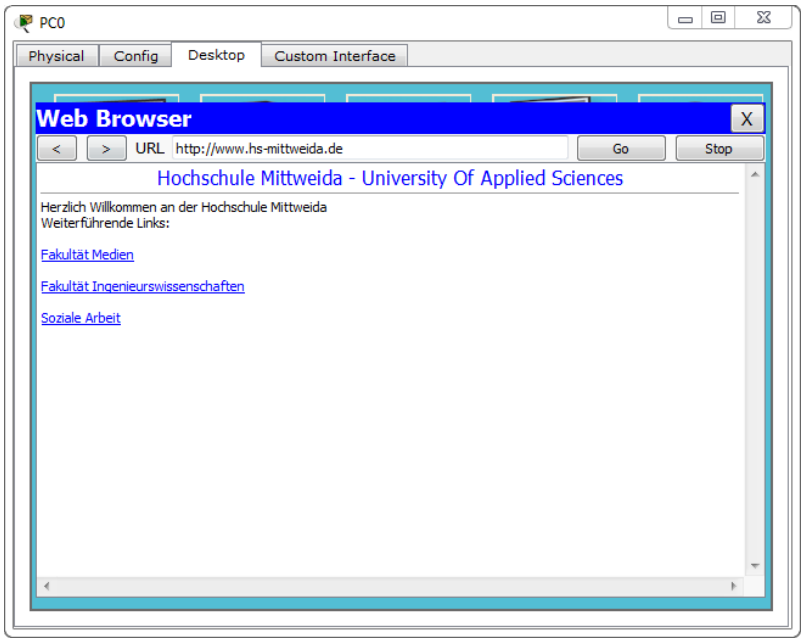

Abbildung 20

Wie Sie sehen, wird die Seite korrekt dargestellt, was die Funktion des DNS Servers bestätigt. Schalten Sie in den Simulationsmodus und rufen Sie erneut die gewünschte URL auf und beobachten Sie, welche Protokolle und Pakete im Hintergrund eines DNS arbeiten.

Aufgabe 3: Einrichtung eines Mailservers

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)	
Generic Server (Standard Server, als DNS – Server)	
2950 – 24 Switch (Standard 24 – Port Switch)	

Diese Aufgabe soll die grundlegende Funktionsweise eines Mailservers demonstrieren. Grundlage für den Emailverkehr ist ein Mailserver, welcher eben

diesen Verkehr steuert. Sämtliche Email – Adressen eines Mailservers erben ihren Domainpart vom Domainnamen des Servers.

Beispiel	
Domain des Mailservers	mail.com
Beispieladresse	name@mail.com

Zum Senden und Empfangen der Emails werden bestimmte Protokolle verwendet. Zu den bekanntesten Protokollen zählen *POP3*[6] und *SMTP*[7]. Diese zwei Protokolle kommen auch im Packet Tracer zur Anwendung. Um den Emailverkehr zwischen Client und Server zu simulieren, bauen Sie zunächst wieder eine Netzwerkumgebung, bestehend aus zwei PCs, einem Switch und einem Server auf. Verbinden Sie die Computer und den Server mit dem Switch und definieren Sie die Netzwerkparameter (IP – Adressen, Subnetzmasken) ordnungsgemäß. Da der Fokus dieser Aufgabe auf der Funktion eines Mailservers liegt, genügt es, diese Netzwerkparameter hier statisch zu vergeben, so dass eine Kommunikation zwischen Clients (PCs) und Server stattfinden kann. Begeben Sie sich im nächsten Schritt in das Konfigurationsfenster des Servers und navigieren Sie unter dem Reiter *Config* in das Untermenü *Email* (Abbildung 21).

[6] POP3 (Post Office Protocol, Version 3) dient hauptsächlich dem Abholen von Emails am Mailserver. Die Funktion des Protokolls ist beschränkt, es kann lediglich Emails abholen, auflisten und löschen. Für die Emailverwaltung in Ordnerstrukturen und Speicherung auf dem Server wird das Protokoll IMAP (Internet Message Access Protocol) verwendet.

[7] SMTP (Simple Message Transfer Protokoll) kann als Gegenstück zu POP3 verstanden werden und dient der reinen Übertragung der Emails vom Absender zum Server und wiederum zum Empfänger.

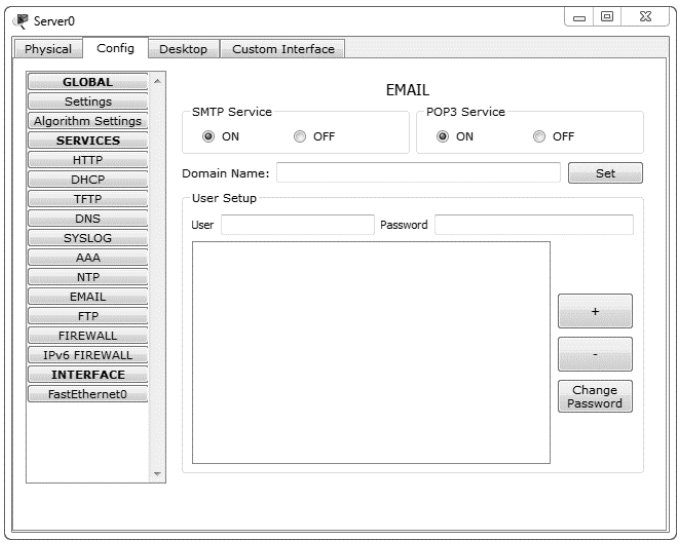

Abbildung 21

Um korrekt zu funktionieren, benötigt der Mailserver zunächst einen *Domain Name*. Wählen Sie hier beispielsweise *mail.com*. Tragen Sie diesen in das dafür vorgesehene Feld ein und speichern Sie per Einfachklick auf *Set* ab. Wie auf einem reellen Mailserver werden Nutzer benötigt, welche in der Nutzertabelle des Servers abgespeichert werden (vgl. Registrierung). An dieser Stelle übernehmen Sie diesen Schritt. Erstellen Sie dazu zwei Nutzer inklusive Passwort und fügen Sie diese mit einem Klick auf das + Symbol der Liste hinzu. Zwei Einträge genügen hier, da sich in dem bestehenden Netzwerk aktuell nur zwei Clients befinden. Stellen sie abschließend sicher, dass die SMTP – und POP3 – Services aktiviert sind. Damit ist die Konfiguration des Mailservers bereits abgeschlossen. Um die Funktion zu testen, begeben Sie sich in die Desktopoberfläche des ersten PCs und öffnen die E-Mail – Applikation per Einfachklick auf *E Mail*. Tragen Sie in das sich nun öffnende Fenster Ihre zuvor eingegebenen Daten ein (Abbildung 22).

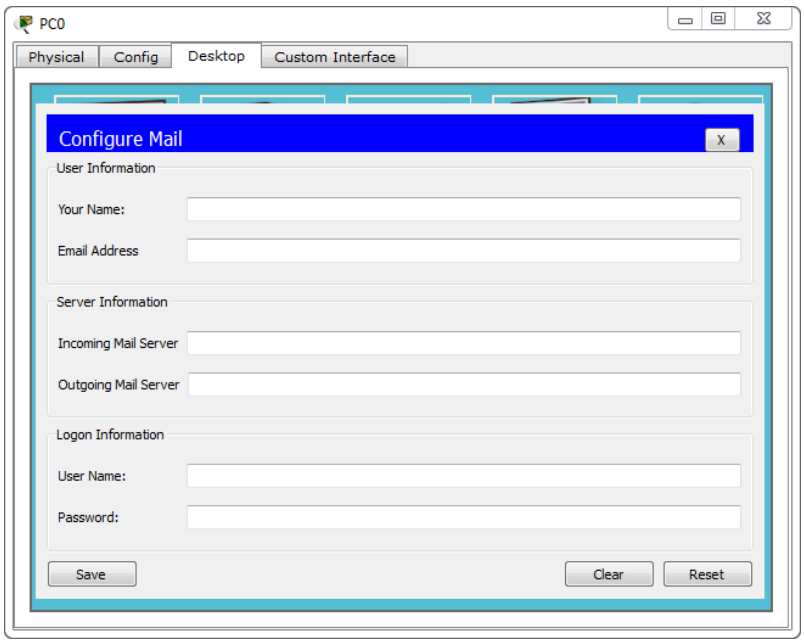

Abbildung 22

Für das Feld *Your Name* können Sie einen beliebigen Namen wählen. Bei *Email Address* müssen Sie den festgelegten Nutzernamen, gefolgt von @ und ihrem gewählten *Domain Name* eintragen.

Beispiel	
Gewählter Domain Name	mail.com
Gewählter User	test
Einzutragende Adresse	test@mail.com

Unter *Incoming*- bzw. *Outgoing Mail Server* geben Sie jeweils die vorher vergebene IP – Adresse des Mailservers an. Abschließend müssen Sie noch die *Logon Information* mit dem entsprechenden Benutzernamen und dem dazugehörigen Passwort ausfüllen (vgl. Anmeldung). Speichern Sie die Daten mittels Einfachklick auf *Save* ab. Sie werden in den Mail Browser weitergeleitet, welcher die Oberfläche eines einfachen E-Mail – Clients darstellt. Wiederholen Sie diese Schritte für den zweiten PC, um diesen ebenfalls für den E-Mail – Verkehr zu konfigurieren.

Nachdem beide Clients korrekt konfiguriert sind, können Sie die Funktion testen. Öffnen Sie dazu erneut die E-Mail – Applikation des ersten PCs. Wählen Sie *Compose*, verfassen Sie eine beliebige E-Mail und versenden Sie diese an den zweiten PC via *Send*. Begeben Sie sich in den *Mail Browser* des anderen PCs und empfangen Sie die zuvor gesendete E-Mail mit Klick auf *Receive*. Waren die vorangegangen Konfigurationen erfolgreich, wird die Nachricht empfangen und kann eingesehen werden (Abbildung 23).

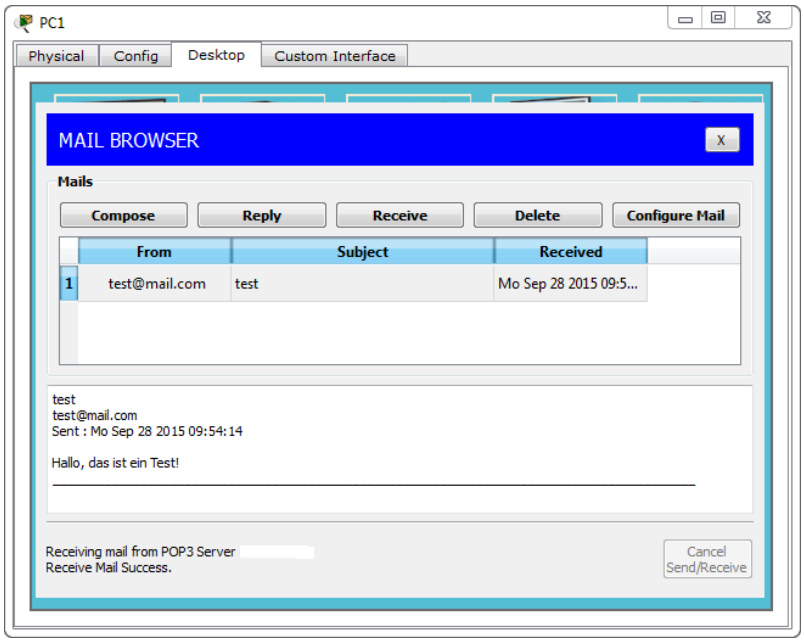

Abbildung 23

Verfolgen Sie im Simulationsmodus (vgl. DHCP – Request) die Vorgänge, welche beim Senden und Empfangen von Mails zwischen Server und Client stattfinden, um ein besseres Verständnis für die Vorgänge zu erhalten, welche schlussendlich dazu führen, dass Emails beim gewünschten Empfänger ordnungsgemäß eingehen.

Aufgabe 4: Kollisionsverhalten innerhalb eines Netzwerkes

Zum Einsatz kommende Hardware:

3 Generic PCs (Standard PC) 

1 Generic Hub (Standard Hub) 

1 2950 – 24 Switch (Standard 24 – Port Switch) 

In diesem Abschnitt soll das Kollisionsverhalten in einem Netzwerk simuliert werden. Dadurch wird zunächst ein Hub als zentrales Übertragungsmedium genutzt und später durch einen Switch ersetzt. Dabei wird demonstriert, welche Auswirkungen eine zeitgleiche Datenübertragung innerhalb eines Hub – Netzwerkes hat und wie diese durch den Einsatz eines Switches umgangen werden können. Es verdeutlicht auch, warum Switches als Nachfolger von Hubs entwickelt wurden und immer häufiger zum Einsatz kamen, bis sie schließlich Hubs vom Markt verdrängt haben. Erstellen Sie zu Beginn ein Netzwerk mit 3 PCs und einem Hub. Verbinden Sie alle PCs mit dem Hub und vergeben Sie geeignete IP – Adressen an alle 3 PCs. Diese müssen sich im selben Netz befinden. Begeben Sie sich in den Simulationsmodus des Programms. Stellen Sie in der Protokollfilterliste ein, dass nur ARP – und ICMP – Pakete angezeigt werden. Um eine Kollision herbeizuführen, schicken Sie eine *Simple PDU* vom ersten PC zum Zweiten. Bevor Sie die Übertragung starten, schicken Sie zusätzlich noch eine *Simple PDU* vom zweiten zum dritten PC (Abbildung 24).

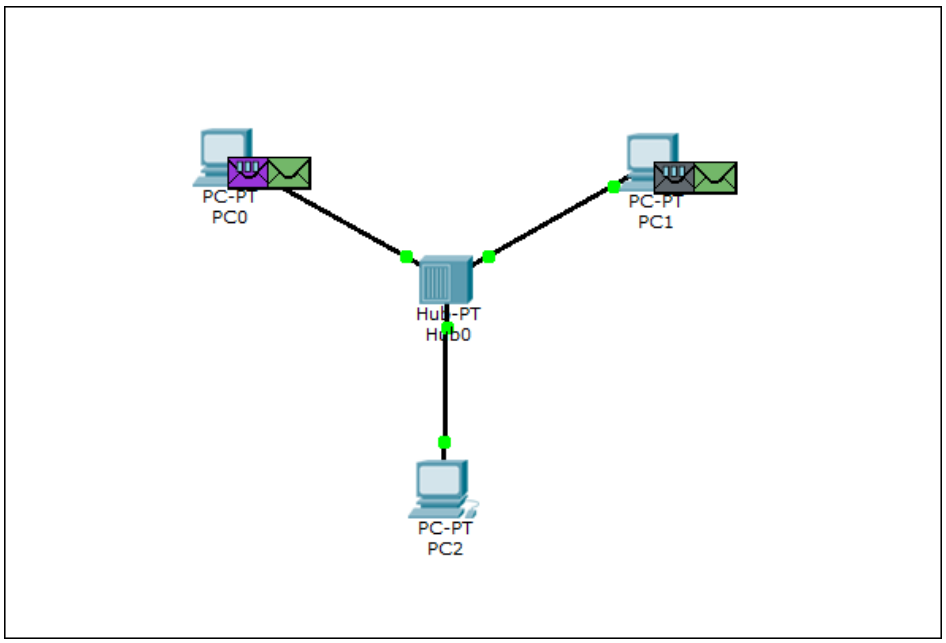

Abbildung 24

Starten Sie die Übertragung mit einem Einfachklick auf *Auto Capture / Play* und beobachten Sie diese. Durch das zeitgleiche Senden der Pakete kommt es bereits im Hub zur Kollision, wie Sie an dem Flammensymbol auf den jeweiligen Paketen erkennen können (Abbildung 25).

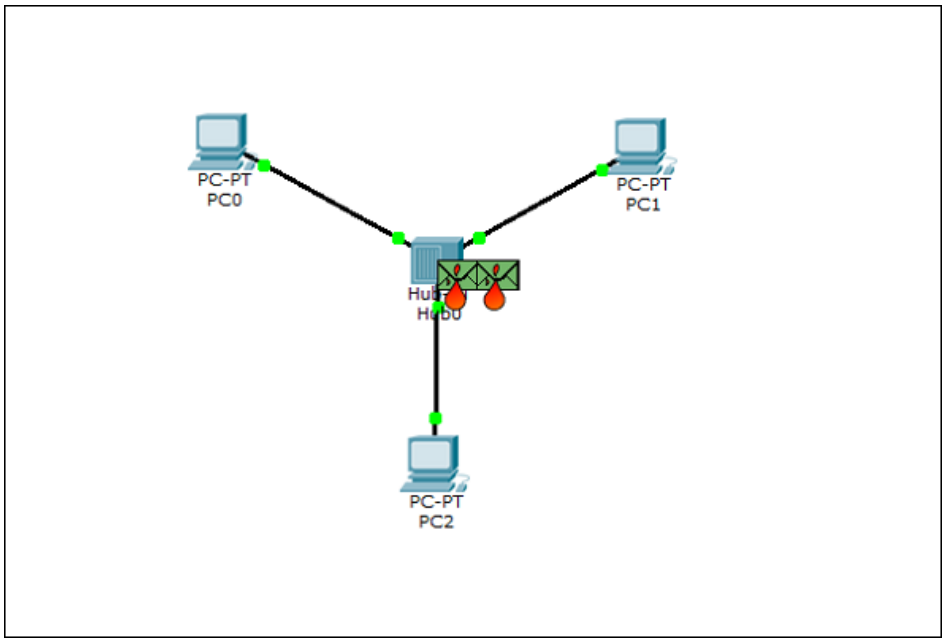

Abbildung 25

Klicken Sie auf einen der beiden Briefsymbole, um sich detailliertere Informationen zum Übertragungsvorgang anzeigen zu lassen. Hier können Sie nachlesen, dass das von Ihnen angeklickte Paket mit einem anderen auf dem Gerät kollidiert ist (Abbildung 26).

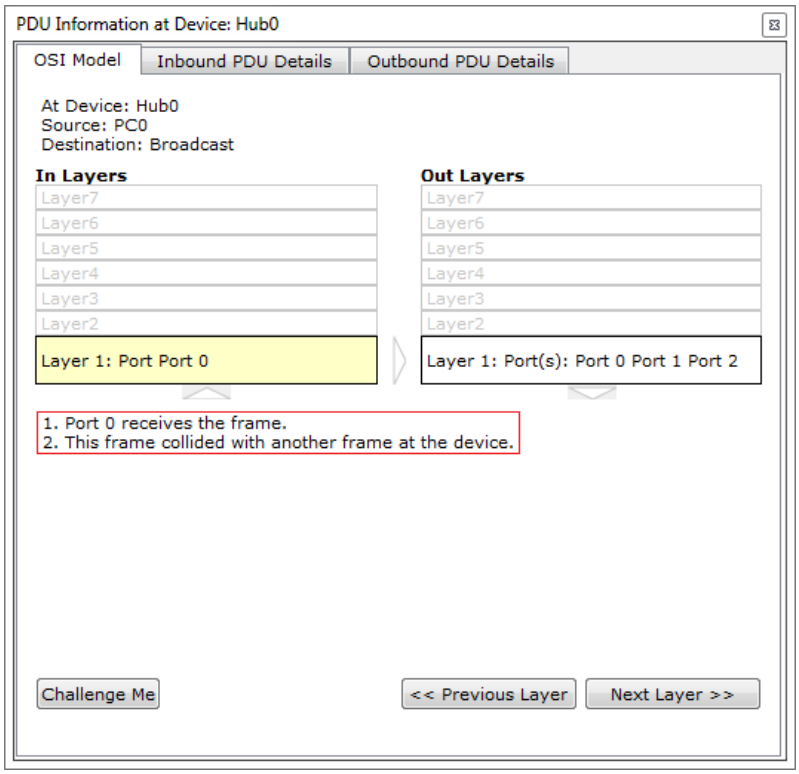

Abbildung 26

Das in der Vorlesung besprochene Verfahren CSMA / CD kommt hier zum Einsatz, um eben jene Kollisionen zu vermeiden (siehe auch Rubrik Zugriffsverfahren, Vorlesungsskript Netzwerktechnik und Administration II). Doch trotz richtiger Handhabung von Kollisionen kosten diese Zeit, u.a. durch die Abhörzeit, die bei CSMA / CD zum Einsatz kommt, um sicherzustellen, dass der zu benutzende Übertragungskanal für die Sendung frei ist und nicht bereits für eine andere Übertragung genutzt wird. Abhilfe für diese Probleme schaffen Switches (im ersten Versuch wurde bereits auf die Funktionsweisen von Hubs / Switches eingegangen). Um die gleichzeitige Paketübertragung mittels eines Switches zu simulieren, tauschen Sie den Hub durch einen 2950 – 24 Switch aus. Der Switch benötigt einige Zeit, um für die Übertragung bereit zu sein. Wechseln Sie in den Echtzeit – Modus und führen Sie einen Einfachklick oberhalb des Geräte Managers auf *Fast Forward Time* aus, um diese Vorbereitungszeit zu verkürzen und wechseln Sie anschließend

wieder zurück in den Simulations – Modus. Starten Sie die Übertragung via Klick auf Auto Capture / Play und beobachten Sie erneut den Sendevorgang. Wie Sie sehen, kommt es nicht zur Kollision, da sich alle über den Switch angeschlossene Geräte nicht mehr auf derselben Kollisionsdomäne befinden. Die Übertragung wird erfolgreich abgeschlossen (Abbildung 27).

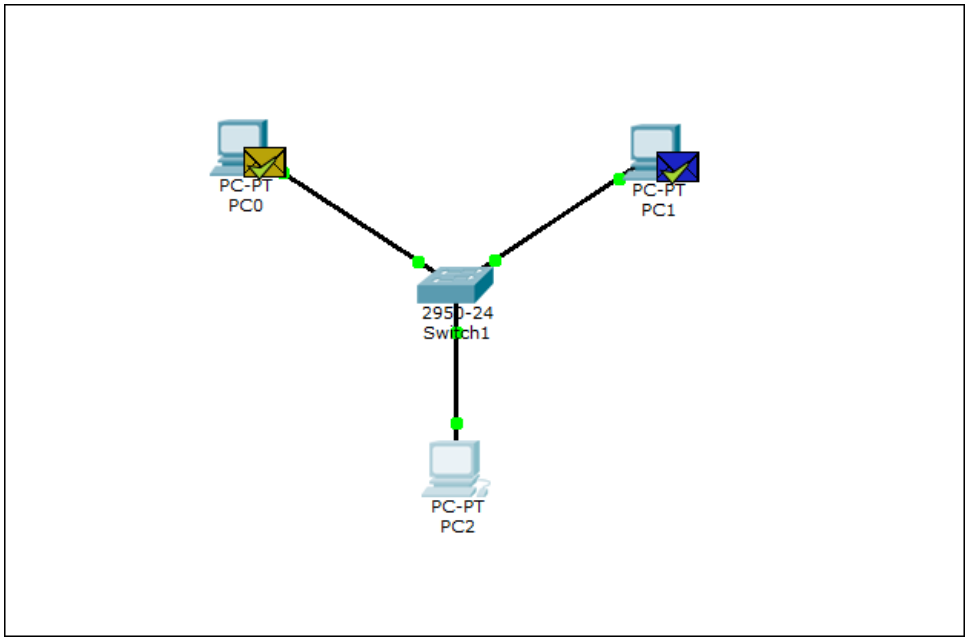

Abbildung 27

Durch den konsequenten Einsatz von Switches wird das CSMA / CD Verfahren überflüssig und die damit verbundenen Probleme hinfällig.

Aufgabe 5: Einrichten eines Netzwerks mit verschiedenen Netzen

Zum Einsatz kommende Hardware:

4 Generic PCs (Standard PC)

2 2950 – 24 Switches (Standard 24 – Port Switch)

1 1841 Router (Standard Cisco – Router)

Bisher basierten alle Aufgaben auf Netzwerkkomponenten, welche sich innerhalb desselben Netzes befinden. Allerdings ist dies in der Praxis nicht umsetzbar,

weshalb es einer Möglichkeit bedarf, eine Kommunikation auch zwischen Geräten zu ermöglichen, welche sich nicht im selben Netz befinden. Hier kommen *Router* zum Einsatz. An dieser Stelle werden Geräte verwendet, welche einzig diesem Zweck dienen (anders, als jene Geräte, die Sie von Zuhause kennen, welche meist Kombigeräte zwischen Switch, Router und Access Point sind und Einschränkungen gegenüber vollwertigen Routern aufweisen).

Um mit Packet Tracer eine Vernetzung zwischen zwei unterschiedlichen Netzen herzustellen, platzieren Sie zunächst 4 PCs auf der Arbeitsfläche. Anschließend verbinden Sie jeweils zwei der eben gesetzten PCs mit einem 2950 – 24 Switch. Vereinfacht handelt es sich bei dieser Konstellation um die zwei verschiedenen Netze. Verbinden Sie die beiden Switches miteinander. Ihr Netzwerk sollte nun wie folgt aussehen (Abbildung 28):

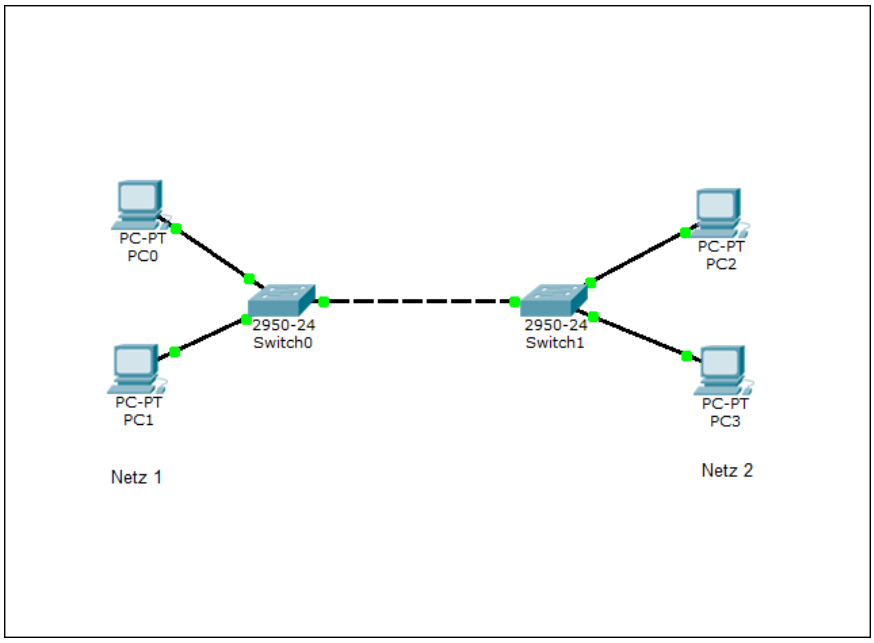

Abbildung 28

In diesem Aufbau wird davon ausgegangen, dass *PC0* und *PC1* zu *Netz 1* und *PC2* und *PC3* zu *Netz 2* gehören. Vergeben Sie Netzwerkparameter an alle 4 PCs. Achten Sie dabei darauf, dass sich *PC0* / *PC1*, sowie *PC2* / *PC3* im selben Netz befinden, diese zwei Netze sich jedoch untereinander unterscheiden müssen. Im Anschluss daran wechseln Sie in den Simulations-Modus des Programms und aktivieren ausschließlich *ICMP* in der Protokollfilterliste. Senden Sie jetzt eine *Simple PDU* von *PC0* an *PC2*. Das Paket wird umgehend verworfen, was Sie an

dem roten Kreuz auf dem Briefsymbol erkennen, welches unmittelbar nach dem Start des Übertragungsvorganges erscheint. Warum das so ist, erfahren Sie, indem Sie einen Einfachklick auf das Briefsymbol ausführen und die detaillierteren Informationen betrachten (Abbildung 29).

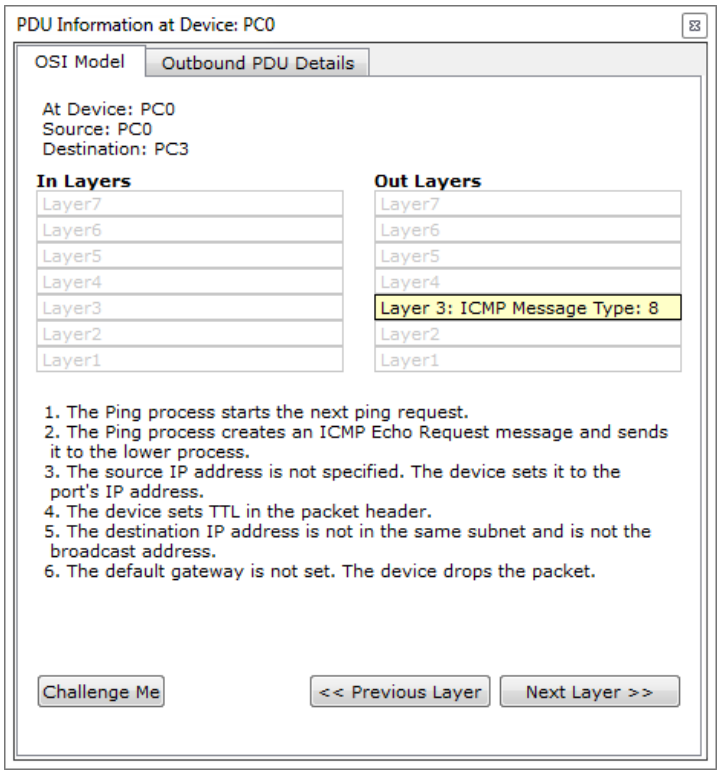

Abbildung 29

Die Übertragung zwischen den beiden Geräten kann nicht funktionieren, da keine Möglichkeit zur Vermittlung zwischen den unterschiedlichen Netzen besteht, in denen sich die PCs befinden. Für diese Aufgabe wird ein Router benötigt. Wählen Sie aus dem Geräte Manager einen 

1841 – Router und platzieren Sie diesen zwischen den beiden Switches und verbinden Sie ihn mit diesen (Abbildung 30).

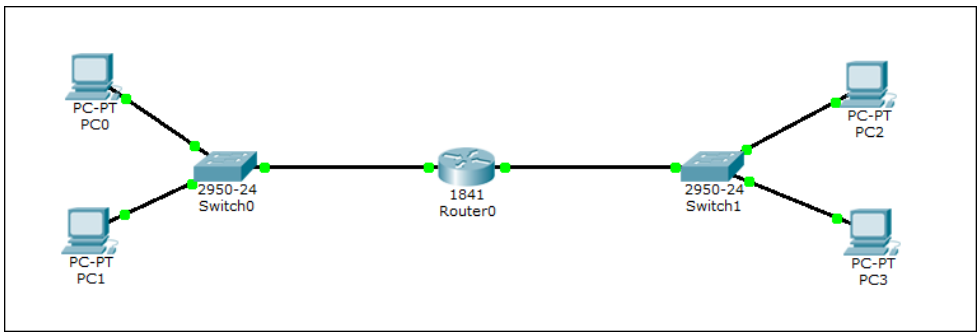

Abbildung 30

Die Aufgabe dieses Routers ist es, Anfragen des einen Netzes in ein anderes Netz weiterzuleiten. Um dies zu ermöglichen, muss der Router beide Netze kennen. Dazu öffnen Sie per Einfachklick auf den Router dessen Konfigurationsoberfläche und wählen den Reiter *Config*. Unter dem Untermenü *Interface* sehen Sie, dass zwei Ethernet – Anschlüsse an diesem Router verfügbar sind, *FastEthernet0/0* und *FastEthernet0/1*. Um in Erfahrung zu bringen, welcher Anschluss mit welchem Ihrer Netze verbunden ist, schließen Sie das Konfigurationsfenster vorerst wieder und fahren Sie mit dem Cursor über einen Anschluss des Routers. Packet Tracer zeigt Ihnen dann den Namen des gewählten Anschlusses an (*Fa0/1* steht hier für *FastEthernet0/1*, Abbildung 31).

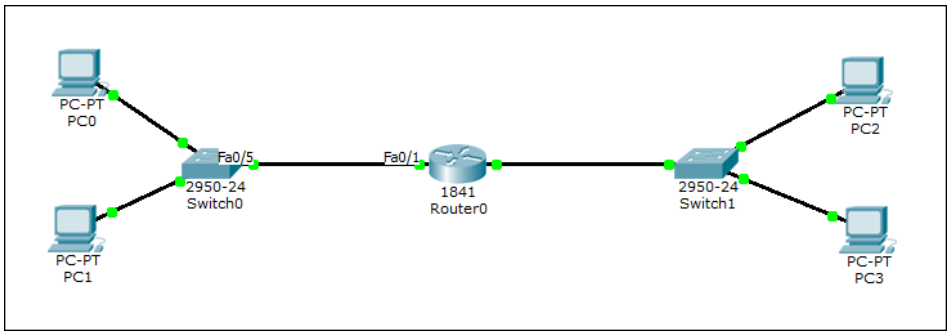

Abbildung 31

Merken Sie sich, welcher Anschluss zu welchem Netzwerk gehört und begeben Sie sich zurück in das Routerkonfigurationsfenster und wählen Sie unter *Config* den Anschluss, an den Ihr erstes Netzwerk angeschlossen ist. Unter *IP Address* und *Subnet Mask* tragen Sie Parameter ein, welche in demselben Netz liegen, wie das jeweilige angeschlossene Subnetz. Die IP – Adresse dieses Anschlusses fungiert

später als *Default Gateway*[8], welches in die IP – Konfiguration der angeschlossenen Geräte im Netzwerk eingetragen wird. Abschließend aktivieren Sie den Anschluss, indem Sie unter *Port Status* das Häkchen setzen. Wiederholen Sie diesen Vorgang für den anderen Anschluss, hier folglich mit Parametern logisch passend zu dem zweiten Netz. Ist dies abgeschlossen, schließen Sie das Konfigurationsfester des Routers. Im nächsten Schritt müssen Sie die verbundenen Geräte mit dem zugehörigen *Default Gateway* „bekanntmachen“. Öffnen Sie dazu nacheinander die IP – Konfiguration der beiden PCs im ersten Netzwerk und tragen Sie unter *Default Gateway* jene IP – Adresse ein, welche Sie dem zugehörigen Anschluss des Routers zugewiesen haben. Diese Einstellung muss für die beiden Computer im zweiten Netz ebenfalls vorgenommen werden, jedoch adäquat zum Routeranschluss dieses Netzes. Das Netzwerk ist fertig konfiguriert und kann getestet werden. Begeben Sie sich dazu erneut in dem Simulations-Modus und wählen Sie im Protokollfilter *ARP*. Schicken Sie anschließend eine *Simple PDU* von einem PC des ersten Netzes an einen PC des zweiten Netzes und verfolgen Sie die Übertragung via Einfachklick auf *Auto Capture / Play*. Bei einer erstmaligen Übertragung zwischen zwei Netzwerkkomponenten wird stets solch ein ARP – Protokoll vorangeschickt, um beider Geräte miteinander „bekannt“ zu machen. Eine kombinierte Übertragung mit *ARP* und *ICMP* ist hier ebenfalls möglich, jedoch für die Übersichtlichkeit ungeeignet. Sollte es nach oder während der Übertragungen zu folgendem Fehler kommen (Abbildung 32) –

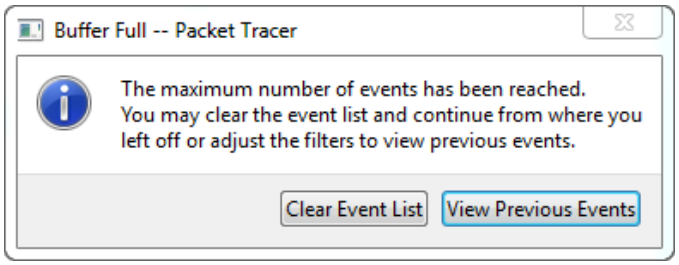

Abbildung 32

– setzen Sie die Simulation via Einfachklick auf *Clear Event List* zurück. Stellen Sie die Protokollfilterliste von *ARP* auf *ICMP* um und verfolgen Sie erneut den Verlauf

[8] Das Default Gateway in einem Netzwerk ist dafür verantwortlich, Pakete aus einem Netz in ein anderes zu übertragen.

des Pakets via *Auto Capture / Play*. War die Konfiguration korrekt, wird das Paket ordnungsgemäß übertragen (Abbildung 33).

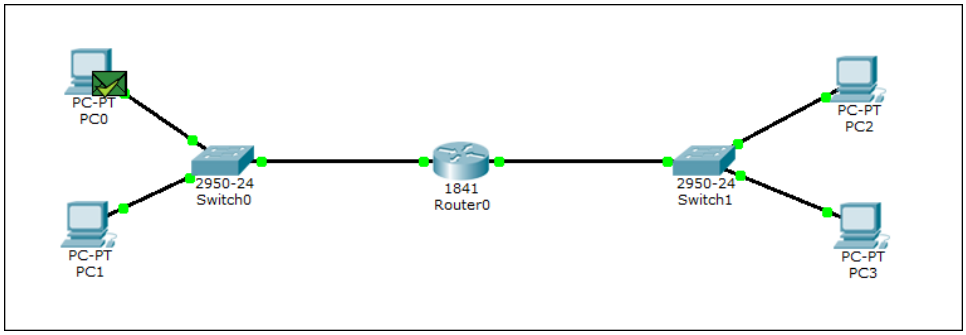

Abbildung 33

Aufgaben zum Versuch

1. Was bedeutet DHCP und wofür wird es benötigt?

2. Wie funktioniert ein DNS – Server?

3. Was ist die Aufgabe eines Routers?

4. Wofür ist das Address Resolution Protocol in IPv4-Netzwerken zuständig?

Lehrgebiet Netzwerktechnik und Administration

Versuch 3: Packet Tracer – Betrachtung weiterer Netzwerktechnologien

Studiengänge	▪ Medientechnik
Ausbildungsziel	▪ Kennenlernen weiterführender Netzwerktechnologien ▪ Verstehen grundlegender Funktionsweisen von verschiedenen Technologien
Ausbildungsinhalte	▪ Einrichtung, Test und Betrachtung von: • MAN • VLAN • Firewalls • NAT ▪ IPv6 ▪ Visualisierung der Paketübertragungswege ▪ Einführung in die Konsolenkonfiguration von Cisco Geräten
Hardware / Software	▪ 1 PC mit Virtual Box inklusive vorinstallierter Packet Tracer Software
Vorkenntnisse	▪ Versuch 1, Versuch 2 ▪ Theoretische Grundlagen der Vorlesungsunterlagen Netzwerktechnik und Administration I & II

In diesem dritten Versuch soll zu Beginn ein einfaches MAN simuliert werden, um die Funktionsweise der Technologie von Netzwerken über einen geografisch ausgedehnteren Raum näher zu betrachten und zu verstehen. Weiterhin sollen mit VLANS eine weitverbreitete und nützliche Technologie simuliert und untersucht werden. Daran anschließend wirft dieser Versuch einen Blick auf den Einsatz und die grundlegenden Funktionsweisen von Firewalls. Aus aktuellem Anlass behandelt dieser Versuch ebenfalls die in der Vorlesung besprochene IPv6 Adressierung. Abschließend soll auf die in der Vorlesung behandelte NAT / NAPT Technologie eingegangen werden, um den theoretischen Grundlagen aus den vorangegangen Versuchen einen praxisnahen Bezug zu vermitteln. Fortführend wird in diesem Praktikum erstmals die IOS – Konsole Anwendung finden, welche in der Praxis zur Konfiguration von Cisco – Routern verwendet wird. Dieser Versuch setzt den Abschluss des ersten und zweiten Versuches voraus, grundlegende Schritte und bekannte theoretische Grundlagen werden in diesem Praktikum nicht mehr Schritt für Schritt erläutert.

Aufgabe 1: Einrichten eines Metropolitan Area Network (MAN) inkl. DHCP

Zum Einsatz kommende Hardware:

6 Generic PCs (Standard PC)	
3 2950 – 24 Switches (Standard 24 – Port Switch)	
3 Generic – Router (zuständig für Routing und DHCP)	
Serial – DCE (Serielles Kabel zur Verbindung der Standorte)	

In diesem Schritt soll unter Verwendung des Packet Tracer ein einfaches *MAN*[1] simuliert werden. Die Aufgabe basiert auf 3 Standorten, deren unterschiedliche Netzwerke über Router miteinander kommunizieren. Diese Technologie wird beispielsweise verwendet, um einzelne Gebäude einer Hochschule miteinander zu vernetzen. In diesem Beispiel sollen pro Standort zwei Clients in Form

[1] MAN (Metropolitan Area Network) ist eine Sonderform des WAN (Wide Area Network). Hierbei werden üblicherweise viele LANs verbunden. Dazu wird meistens eine Glasfasertechnik verwendet.

handelsüblicher Computer ans Netz angeschlossen werden. Die Clients sind miteinander über einen Switch verbunden, welcher wiederum am zugehörigen Router angeschlossen wird. Dieser Router übernimmt ebenfalls die IP – Vergabe via DHCP für den betreffenden Standort.

Zu Beginn platzieren Sie zunächst für jeden der 3 Standorte die Clients auf der Arbeitsfläche. Setzen Sie ebenfalls zu jeder Zweiergruppe PCs einen Standard *2950 – 24 Switch* dazu (Abbildung 1).

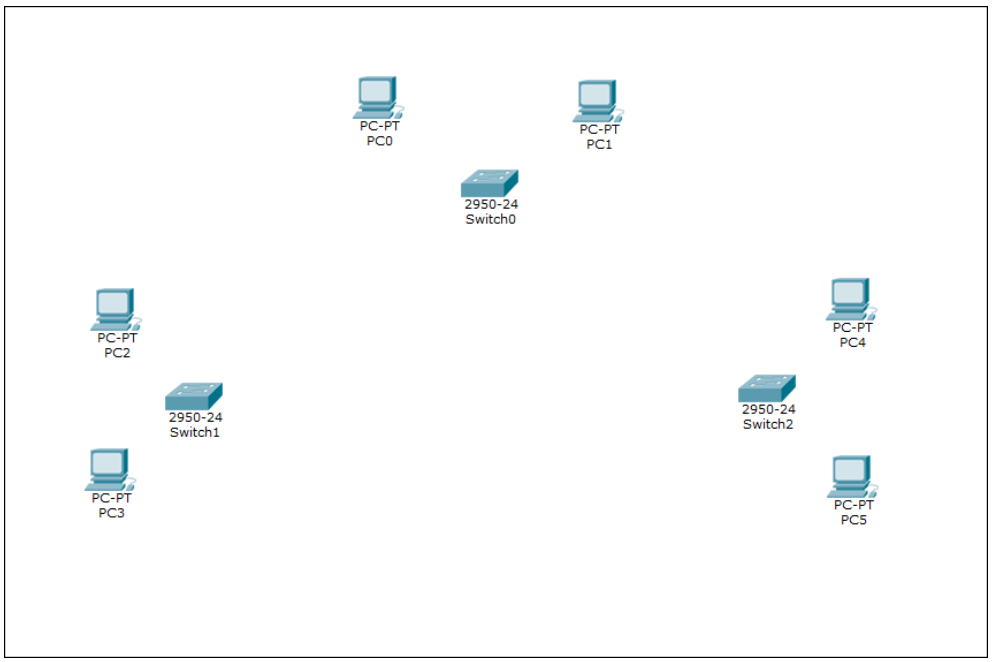

Abbildung 1

Verbinden Sie diese Komponenten wie gewohnt. Lassen Sie jedoch den Anschluss *FastEthernet0/24* am Switch unbelegt, da dieser für die Verbindung zum Router genutzt werden soll. Im nächsten Schritt wählen Sie die Router aus. Benutzen Sie für diese Konstellation 

3 Generic – Router. Achten Sie dabei darauf, dass Sie im Geräte – Manager *Router-PT* und nicht *Router-PT-Empty* wählen (Abbildung 2).

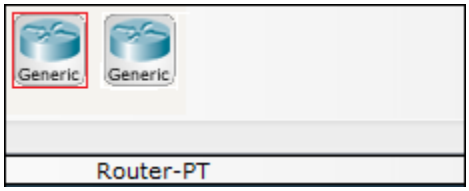

Abbildung 2

Fügen Sie anschließend jeweils einen *Generic – Router* zu jedem Netz hinzu (Abbildung 3).

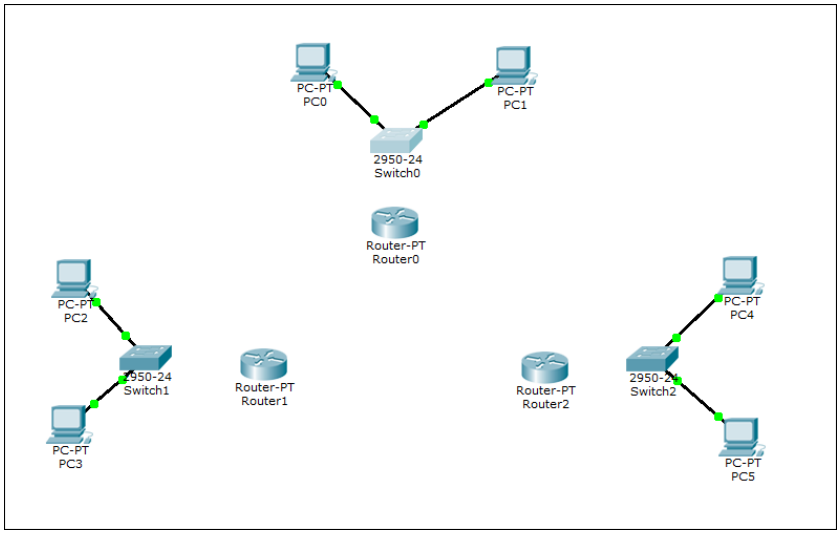

Abbildung 3

Dieser Router verfügt im Vergleich zu den bisherig benutzten Routern über serielle Anschlüsse, welche für die Verbindung der einzelnen Standorte notwendig sind. Verbinden Sie jeden Switch mit dem dazugehörigen Router. Zur besseren Übersichtlichkeit, verwenden Sie an den Routern jeweils den *FastEthernet0/0* – Port. An den Switches nutzen Sie dazu den zuvor freigehaltenen Port *FastEthernet0/24* (Abbildung 4).

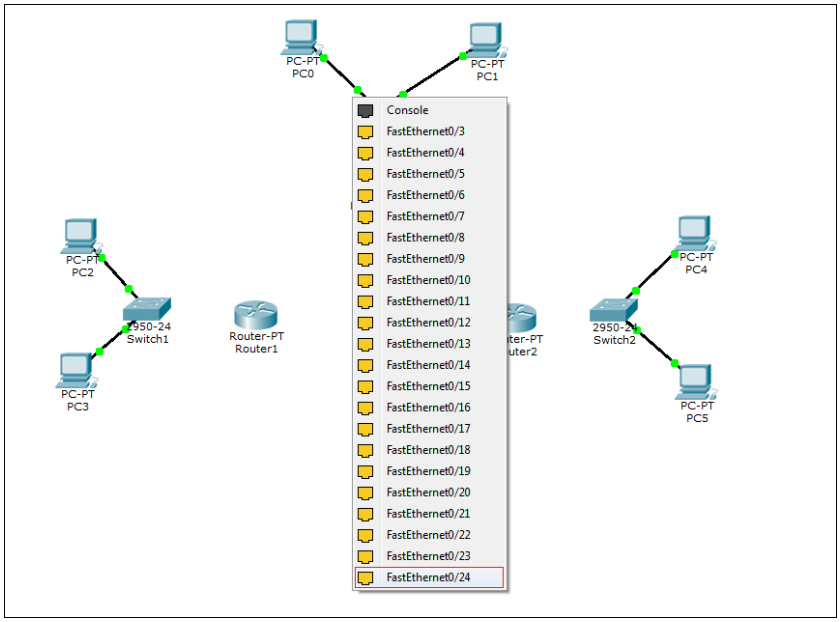

Abbildung 4

Abschließend wählen Sie im Gerätemanager  *Serial DCE*. Hierbei handelt es sich um ein serielles Kabel, welches besonders zur Datenübertragungen über große Entfernungen und somit zur Verbindung der 3 Standorte in diesem Versuch geeignet ist. Verbinden Sie die Router über die Serial - Ports (Abbildung 5).

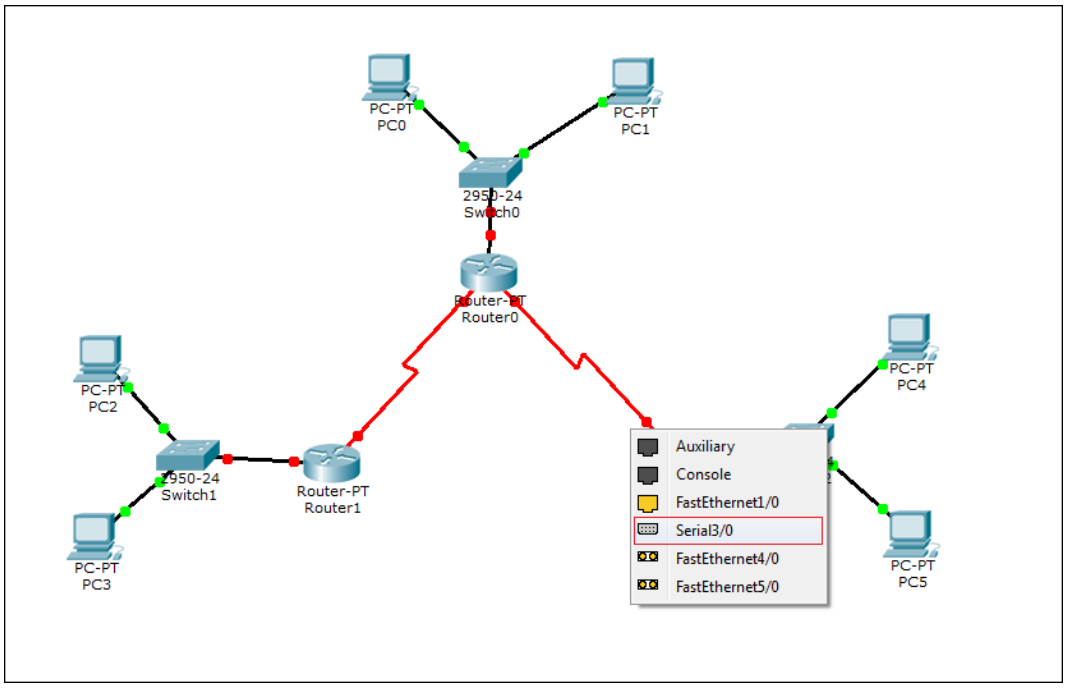

Abbildung 5

Das Grundgerüst des Netzwerks ist nun fertiggestellt. In den nächsten Schritten wird die Konfiguration des Netzwerkes näher betrachtet. Folgende Netze sollen für die Clients verwendet werden:

Erstes Netz	*192.168.1.x*
Zweites Netz	*192.168.2.x*
Drittes Netz	*192.168.3.x*

Da eine statische IP – Vergabe an die Clients eines Netzwerkes in der Praxis unüblich ist, soll diese hier dynamisch stattfinden. Damit die Router diese Aufgabe übernehmen können, müssen diese per Konsole auf diesen Dienst programmiert werden. Bevor jedoch auf diese Konfiguration näher eingegangen wird, bedarf es noch einiger Einstellungen. Zunächst müssen die Gateways der Router definiert werden, damit eine Kommunikation der Netze untereinander gewährleistet ist. Hier soll gelten, dass jenes Gateway des Routers eines Netzes jeweils die letzte IP –

Adresse in diesem erhält (Beispiel: Netz 1, Gateway 192.168.1.254). Setzen Sie für die verwendeten FastEthernet – Ports der Router diese Gateways. Orientieren Sie sich an der Bezeichnung der Geräte, um eine geordnete Reihenfolge zu erhalten (Abbildung 6).

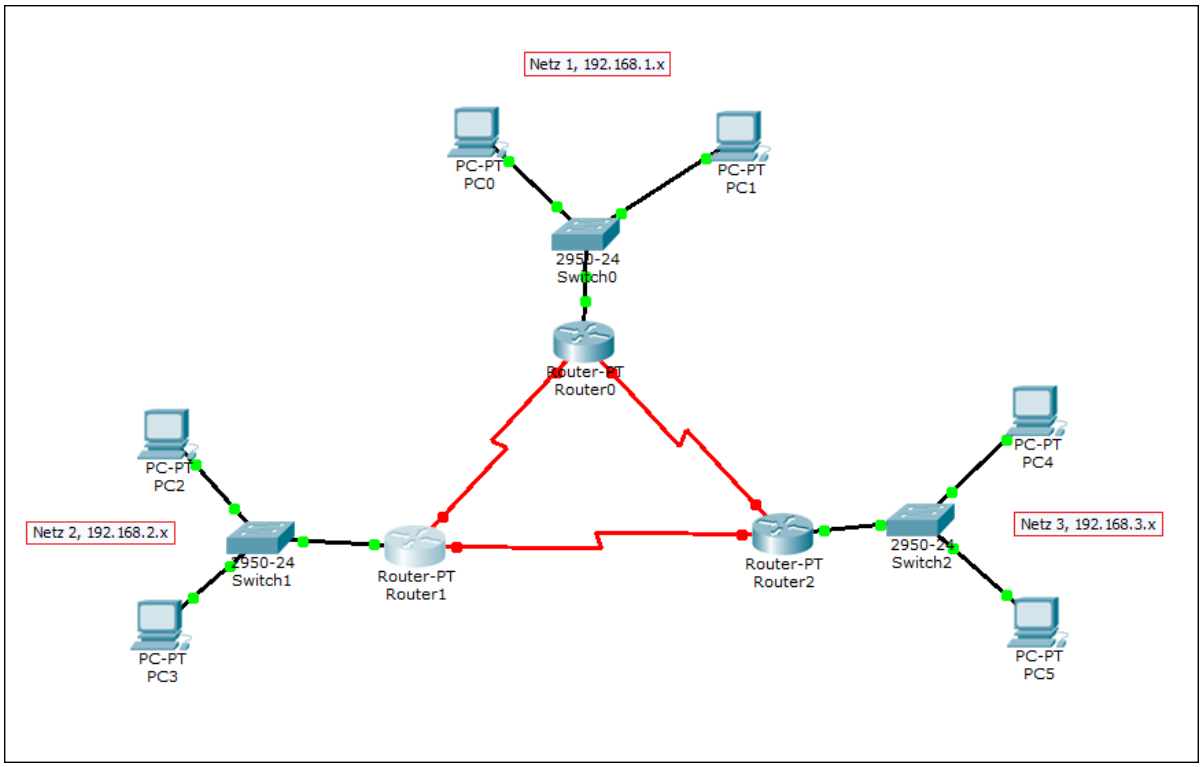

Abbildung 6

Achten Sie darauf, nach der Zuweisung der IPs den Port – Status des betreffenden Anschlusses auf *On* zu schalten. Bei Problemen mit dieser Konfiguration, orientieren Sie sich an *Versuch 2, Aufgabe 4: Einrichten eines Netzwerks mit verschiedenen Netzen.* Damit sind die Gateways auf Seite des Clients konfiguriert. In einem nächsten Schritt soll die IP – Vergabe an die Clients per DHCP auf den Routern eingerichtet werden. Dies findet in der IOS – Konsole (*IOS Command Line Interface, CLI*) statt. Rufen Sie diese über den Reiter *CLI* im Konfigurationsfenster *Router0* auf (Abbildung 7).

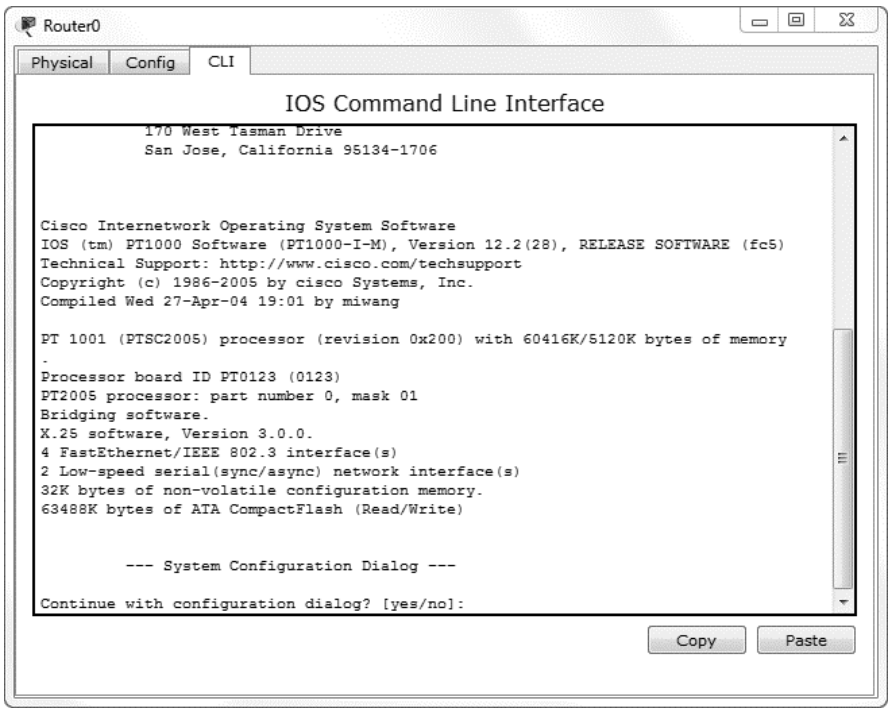

Abbildung 7

Continue with configuration dialog? gibt Ihnen die Möglichkeit, den Router per Kommandozeile in einem Basic Setup zu konfigurieren (IP – Adresse, Subnetzmaske usw.). Dies soll an dieser Stelle ohne Bedeutung sein. Tippen Sie ein *no* in die Kommandozeile und bestätigen Sie dies mit *Enter* (Abbildung 8).

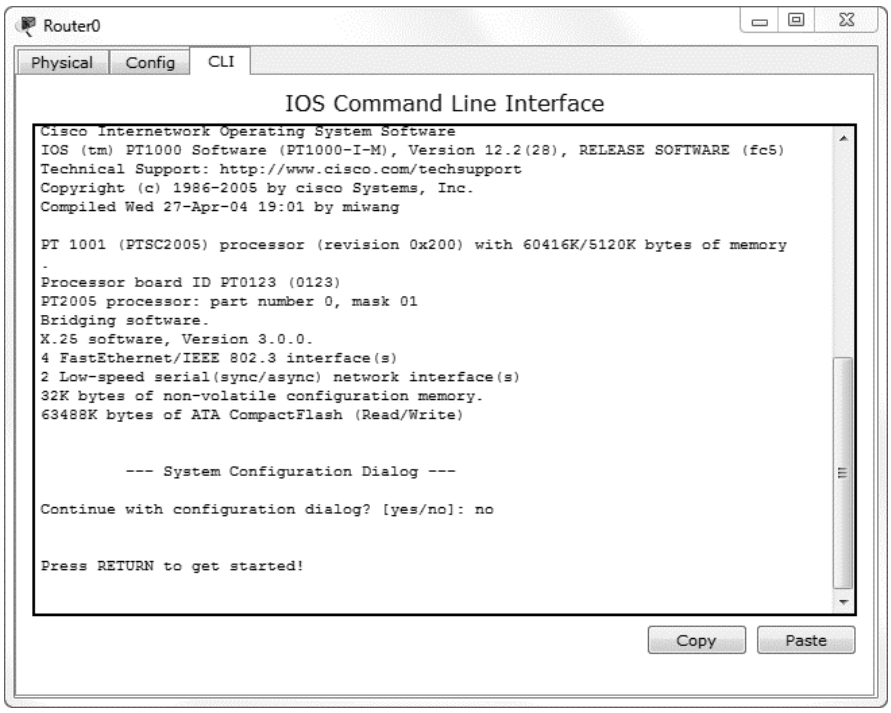

Abbildung 8

Durch erneutes Betätigen der *Enter* – *Taste* starten Sie die manuelle Konfiguration (Abbildung 9).

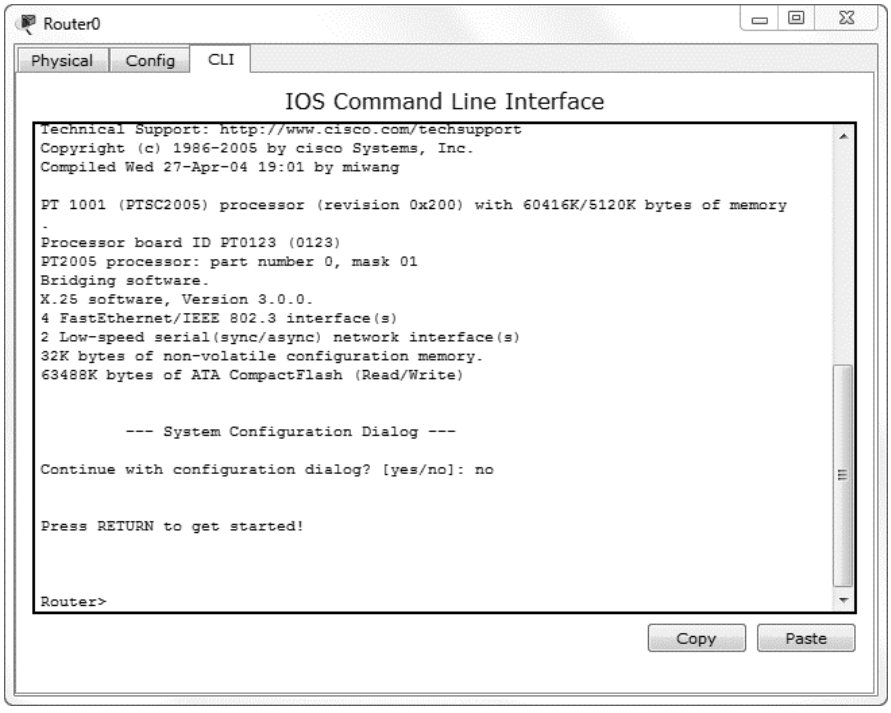

Abbildung 9

Den Router bereiten Sie mit dem Befehl

enable

auf die Konfiguration vor. Senden Sie den Befehl mit *Enter* ab. Mit einer nächsten Eingabe

configure terminal

verschaffen Sie sich Zugang zum globalen Konfigurationsmodus. Da der Router bereits eine eine statische IP zugewiesen bekommen hat, müssen Sie diese zunächst von der IP – Vergabe ausschließen. Geben Sie den folgenden Befehl

ip dhcp excluded-address 192.168.1.254

in die Konsole ein und bestätigen Sie erneut mit *Enter*. Damit ist das Gerät darauf programmiert, diese IP bei der Zuweisung nicht zu berücksichtigen. Durch die Eingabe

ip dhcp pool [beliebiger Name Ihres Netzes][2]

begeben Sie sich in die DHCP Konfiguration des Routers. An der aktuellen Pfadangabe der Konsole *Router (dhcp-config)* ist erkennbar, dass man sich in der DHCP – Konfiguration befindet. Durch den Befehl

network 192.168.1.0 255.255.255.0

teilen Sie dem Router mit, dass dieser an alle an diesen Router angeschlossenen Geräte, die einen DHCP – Request senden, eine IP Adresse aus dem *192.168.1.x* – Netz vergibt. Damit alle Pakete, welche in die anderen Netze gesendet werden sollen, erfolgreich über diesen Router vermittelt werden können, muss dieser in einem nächsten Schritt als *Default Gateway* konfiguriert werden. Dies wird durch die Eingabe des Befehls

default-router 192.168.1.254

erreicht. Die Konfiguration ist jetzt abgeschlossen und Sie können die DHCP – Konfiguration durch Eingabe von *exit* verlassen. Die vollständige Konfiguration von *Router0* in *Netz 1* über die Konsole sollte wie folgt aussehen (Abbildung 10):

[2] Angabe ohne [ ]

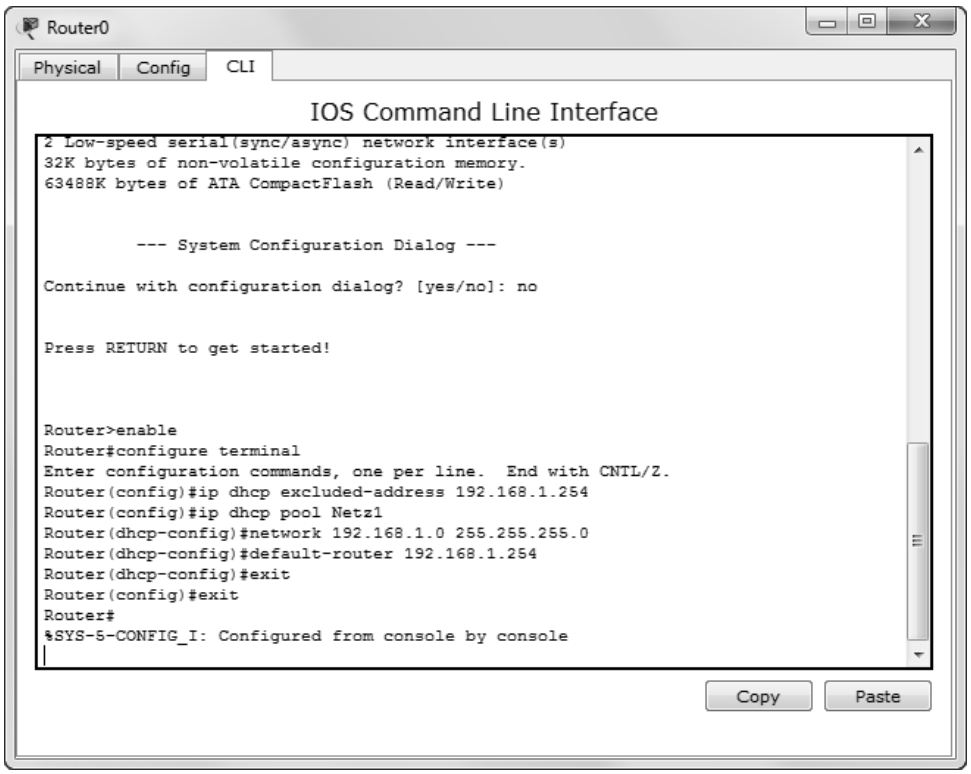

Abbildung 10

Schließen Sie das Konsolenfenster. Um die einwandfreie Funktion der eben konfigurierten DHCP – Zuweisung zu überprüfen, öffnen Sie das Einstellungsfenster von *PC0* und wählen im Reiter Desktop das Menü *IP Configuration*. Aktivieren Sie den DHCP – Modus. Sind alle Schritte korrekt ausgeführt worden, erhält der PC nun die erste freie IP aus dem von Ihnen festgelegten IP – Pool (Abbildung 11).

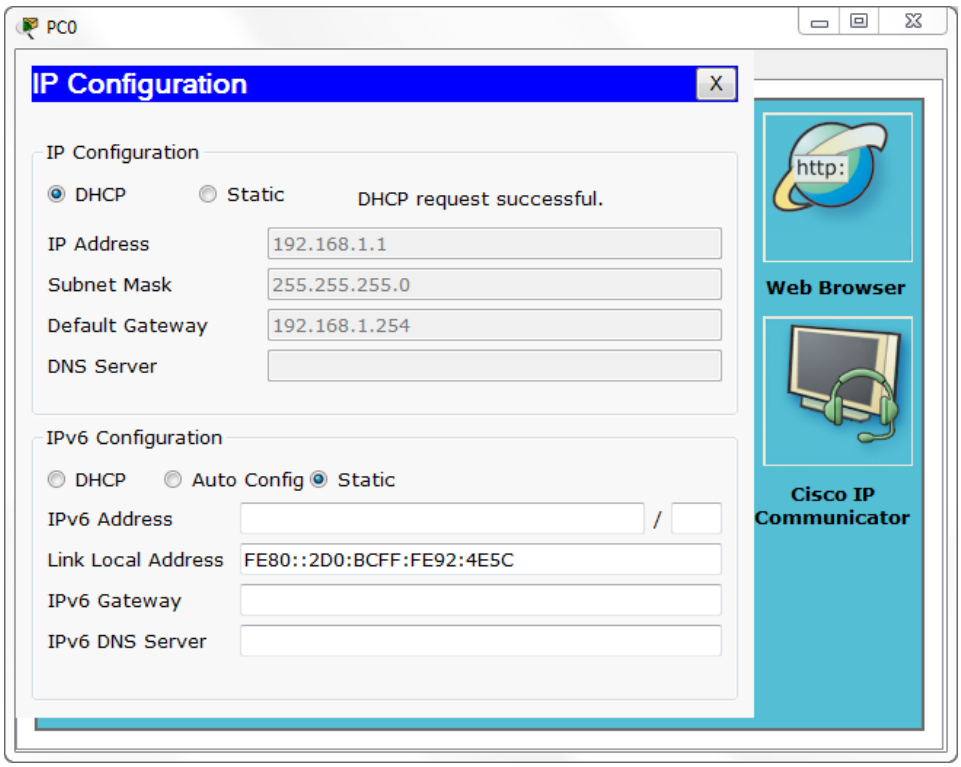

Abbildung 11

Ein DNS Server findet in diesem Beispiel keine Anwendung. Dieser kann jedoch im Falle einer Verwendung innerhalb der DHCP – Konfiguration über den Befehl

dns-sever (IP Adresse des DNS – Servers)

hinzugefügt werden.

Wiederholen Sie diese Schritte zur Konfiguration der anderen beiden Router, um diese für die IP – Vergabe in den zugehörigen Netzen zu programmieren. Ist dies abgeschlossen, müssen Sie abschließend bei sämtlichen beteiligten PCs die IP – Bezugsmethode auf DHCP stellen, damit jedes Gerät eine IP erhält. Vergewissern Sie sich, dass alle Komponenten eine IP erhalten, um Fehler bei der Konfiguration auszuschließen.

Im nächsten Schritt muss eine Kommunikation zwischen den Router gewährleistet werden. Dazu müssen die seriellen Anschlüssen ebenfalls noch konfiguriert werden. Rufen Sie dazu das Konfigurationsfenster von *Router0* auf und begeben Sie sich unter *Config* / *Interfaces* ins Untermenü des Anschlusses, welcher zur Verbindung mit *Router1* verbunden ist. Sollten Sie sich nicht erinnern, über welche Anschlüsse die Router verbunden sind, schließen Sie das Konfigurationsfenster

und berühren Sie mit dem Cursor den betreffenden Anschluss, um sich die Bezeichnung des Ports anzeigen zu lassen (siehe auch *Abbildung 24, Versuch 2*). Zurück im Menü tragen Sie folgende Daten ein:

IP Address	*10.30.101.1*
Subnet Mask	*255.255.255.0*

Vergewissern Sie sich auch, dass der Port Status auf *On* geschaltet ist. Dieser erste Port ist nun konfiguriert und Sie können das Fenster schließen. Begeben Sie sich in das Einstellungsmenü des zugehörigen Ports in *Router1*. Hier fügen Sie folgende Parameter ein:

IP Address	*10.30.101.2*
Subnet Mask	*255.255.255.0*

Verfahren Sie mit allen noch übrigen seriellen Anschlüssen der Router genauso. Nehmen Sie dazu folgende Tabelle bzw. Abbildung 12 zur Hilfe:

Router1, Interface verbunden mit Router2	IP Adresse	*10.30.102.1*
	Subnetzmaske	*255.255.255.0*
Router2, Interface verbunden mit Router1	IP Adresse	*10.30.102.2*
	Subnetzmaske	*255.255.255.0*
Router2, Interface verbunden mit Router0	IP Adresse	*10.30.103.1*
	Subnetzmaske	*255.255.255.0*
Router0, Interface verbunden mit Router2	IP Adresse	*10.30.103.2*
	Subnetzmaske	*255.255.255.0*

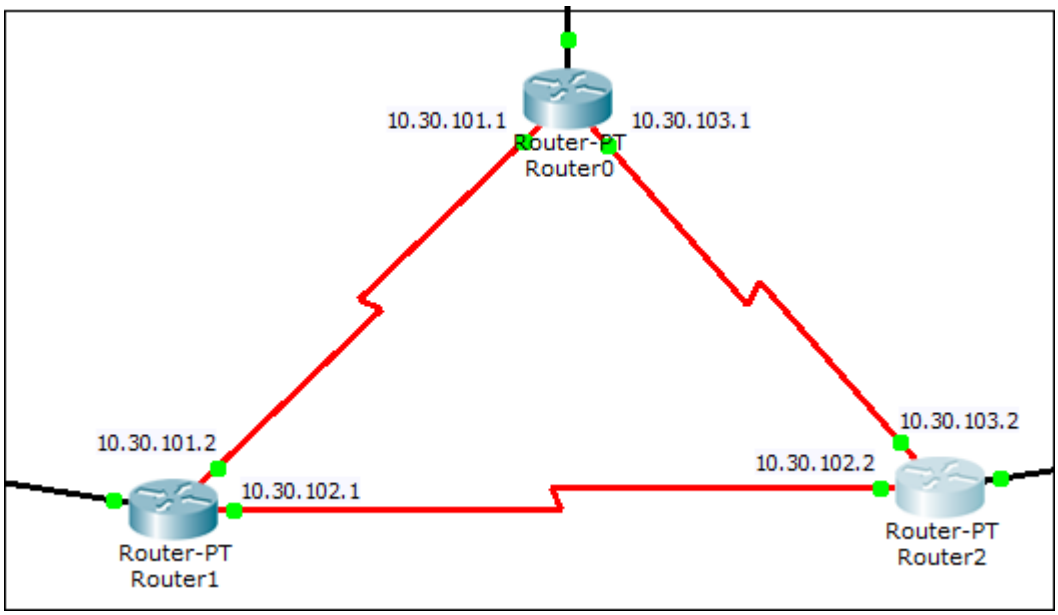

Abbildung 12

Nach Abschluss dieser Einstellungen wählen Sie bitte eine *Simple PDU* und schicken Sie diese von *PC0* an einen PC Ihrer Wahl in einem der beiden anderen Netze. Wie Sie sehen, schlägt diese Übertragung fehl. Dies liegt daran, dass die Router zwar eine Adresse besitzen, aber noch nicht zwischen diesen kommunizieren können. Dazu muss den Routern noch mitgeteilt werden, welche Netzwerke über welche Ports erreichbar sind (*Routing*). Um die erste Verbindung zwischen Netz 1 und Netz 2 zu vervollständigen, rufen Sie das Menü *Static*[3] (statische Route) über den Reiter *Config* im Konfigurationsfenster von Router0 auf (Abbildung 13).

[3] Statische Routen werden per Hand vom Administrator in die Tabelle eingetragen.

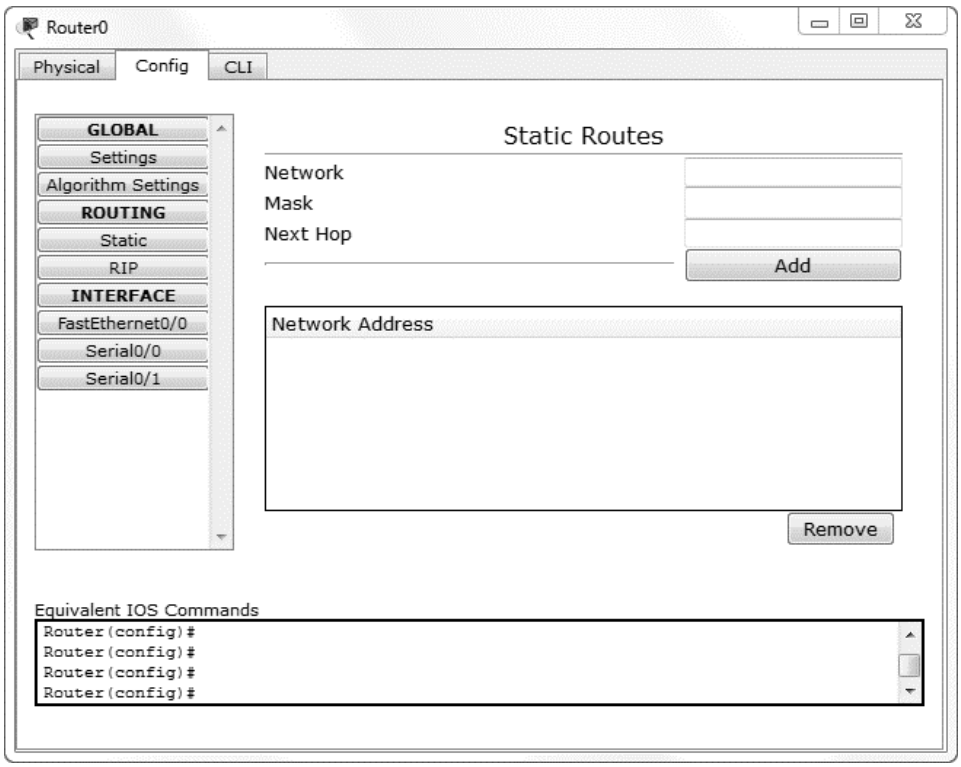

Abbildung 13

In jedem Router müssen hier jeweils zwei IP – Routen definiert werden, jedes Gerät in diesem Beispiel an zwei Netze angeschlossen ist. Widmen Sie sich zuerst der Verbindung zu Netz 2 (192.168.2.x). Tragen Sie folgende Parameter in die dafür vorgesehenen Felder ein:

Network	*192.168.2.0*
Mask	*255.255.255.0*
Next Hop[4]	*10.30.101.2*

Fügen Sie den Eintrag per Einfachklick auf *Add* zur Routingliste hinzu. Wie an diesen Parametern erkennbar ist, sind als Route jeweils die Daten des zu kontaktierenden Netzes einzutragen. Wechseln Sie in das *Static* – Menü von *Router1* und schließen Sie die Verbindungskonfiguration zu Netz 1 ab. Fügen Sie hier die Route hinzu, welche Netz 1 kontaktiert:

[4] Next Hop definiert den nächsten Netzknoten, zu welchem das zu vermittelnde Paket übertragen werden muss. Hier ist der jeweilige serielle Port gemeint, über welchem die Router miteinander verbunden sind.

Network	*192.168.1.0*
Mask	*255.255.255.0*
Next Hop	*10.30.101.1*

Führen Sie diese Schritte angepasst an allen Routern durch und bringen Sie somit die Konfiguration Ihres MANs zum Abschluss. Das aufgebaute und eingerichtete MAN könnte so beispielsweise zur Vernetzung verschiedener Firmengebäude oder der zahlreichen Häuser einer Hochschule innerhalb einer Stadt verwendet werden (Abbildung 14).

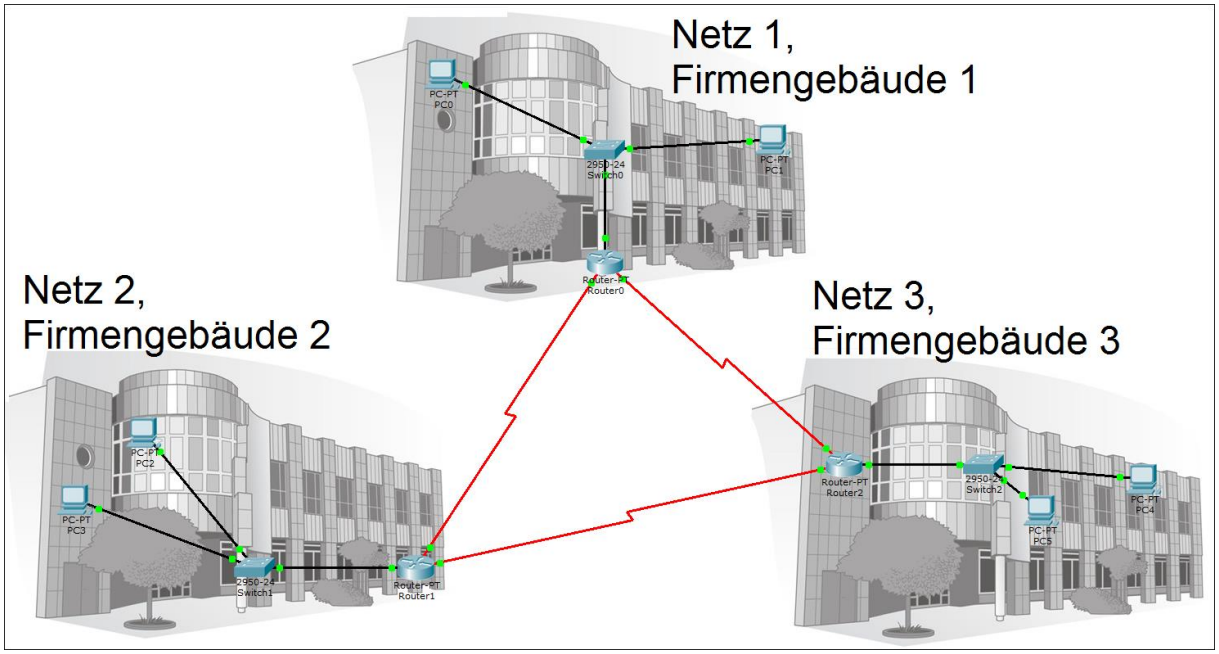

Abbildung 14

Testen Sie die Kommunikation der angeschlossenen Netzwerkkomponenten untereinander. Denken Sie auch hier daran, dass die jeweils erste Übertragung einer PDU zwischen zwei Komponenten durch den ARP – Request fehlschlagen kann. Sollte dies bei Ihnen auftreten, starten Sie erneut eine Übertragung zwischen diesen beiden Komponenten. Leeren Sie vorher bei Bedarf die Eventliste.

Aufgabe 2: Einrichten eines VLANs mit statischer IP – Vergabe

Zum Einsatz kommende Hardware:

12 Generic PCs (Standard PC) 

2 2950 – 24 Switches (Standard 24 – Port Switch) 

In dieser nächsten Aufgabe soll ein funktionsfähiges *VLAN*[5] eingerichtet und die grundlegende Funktion mit Hilfe der Packet Tracer Simulation verstanden werden. VLANs kommen beispielsweise in größeren Unternehmen zum Einsatz, welche ein physikalisches Netz besitzen, in diesem jedoch Abteilungen untereinander in virtuelle Teilnetze aufgeteilt sind. Dadurch ist eine Kommunikation der Fachbereiche ausschließlich untereinander gewährleistet. Man unterscheidet zwischen *statischen*, *dynamischen* und *tagged* VLANS. Diese Aufgabe basiert auf dem Prinzip des statischen VLANS, in welchem bestimmte Ports des Switches einem, vom Administrator festgelegten VLAN angehören. In diesem Beispiel sollen 3 VLANs eingerichtet werden, welche über einen Switch gesteuert werden (vgl. beispielsweise 3 Fachbereiche einer Firma auf einer Etage des Firmengebäudes). Darauf aufbauend soll noch ein weiterer Switch installiert werden, welcher über einen *Trunk*[6] mit dem Ausgangsswitch verbunden ist (vgl. zum Beispiel die genannten Fachbereiche auf unterschiedlichen Etagen des Firmengebäudes). Zum Aufbau des ersten einfachen VLANs platzieren Sie zunächst einen handelsüblichen 24 – Port Switch mittig auf der Arbeitsfläche. Um den eben platzierten Switch setzen Sie insgesamt 12 PCs, jeweils in Zweiergruppen zusammengefasst. Verbinden Sie die Computer mit dem Switch. Die Konstellation sollte etwa wie folgt aussehen (Abbildung 15):

[5] Als VLANs (Virtual Local Area Network) werden virtuelle Teilnetze eines physikalischen Netzes bezeichnet.
[6] Als Trunk wird eine physikalische Leitung bezeichnet, welche mehrere Übertragungskanäle (hier VLANs) zu einer logischen Verbindung zusammenführt.

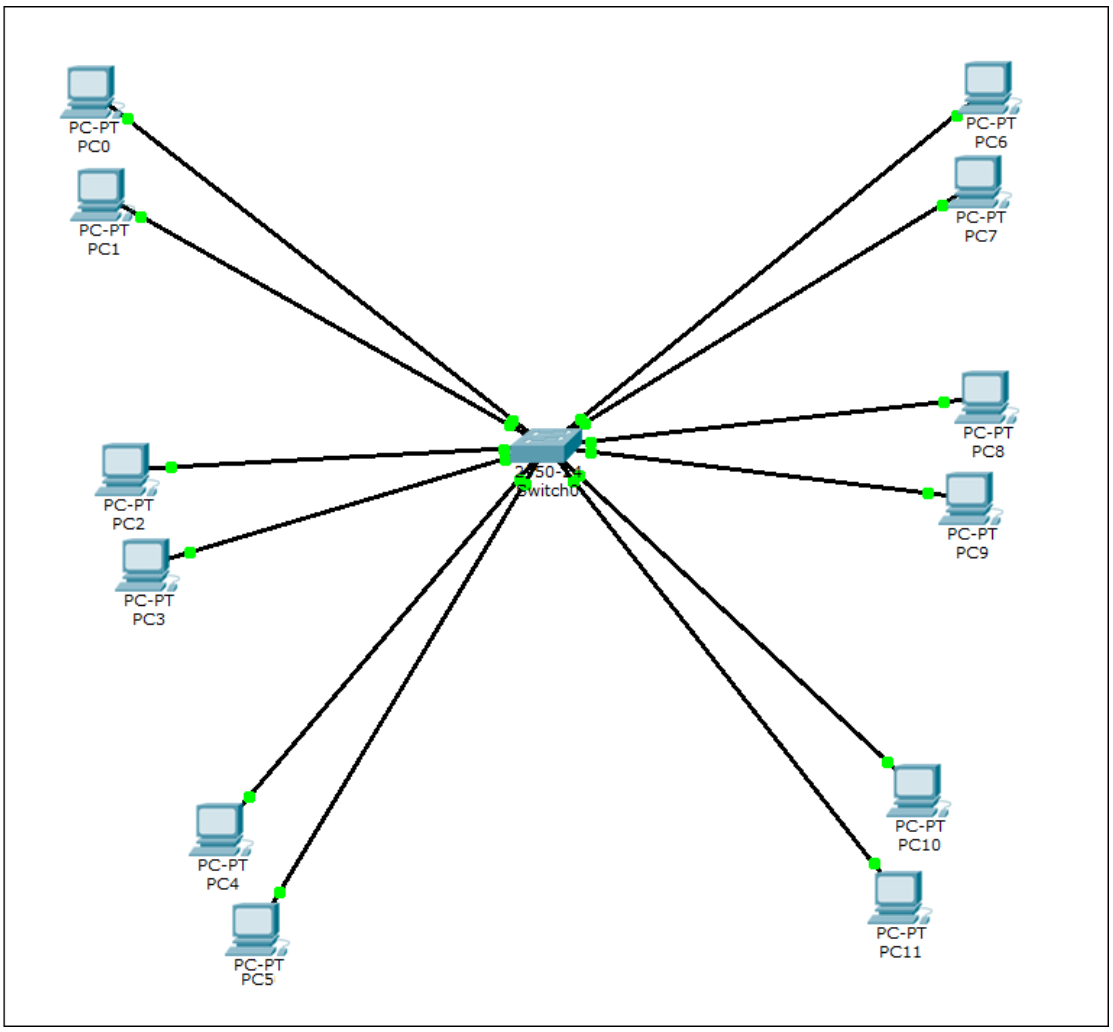

Abbildung 15

Konfigurieren Sie für jeden PC die IP Einstellungen. Achten Sie darauf, dass sich sämtliche Computer im gleichen Netz befinden sollen, da auf Routing an dieser Stelle verzichtet werden soll. Im nächsten Schritt soll sich der VLAN – Konfiguration zugewandt werden. Öffnen Sie dazu die Konfigurationsübersicht des Switches und navigieren Sie über Config nach VLAN Database (Abbildung 16).

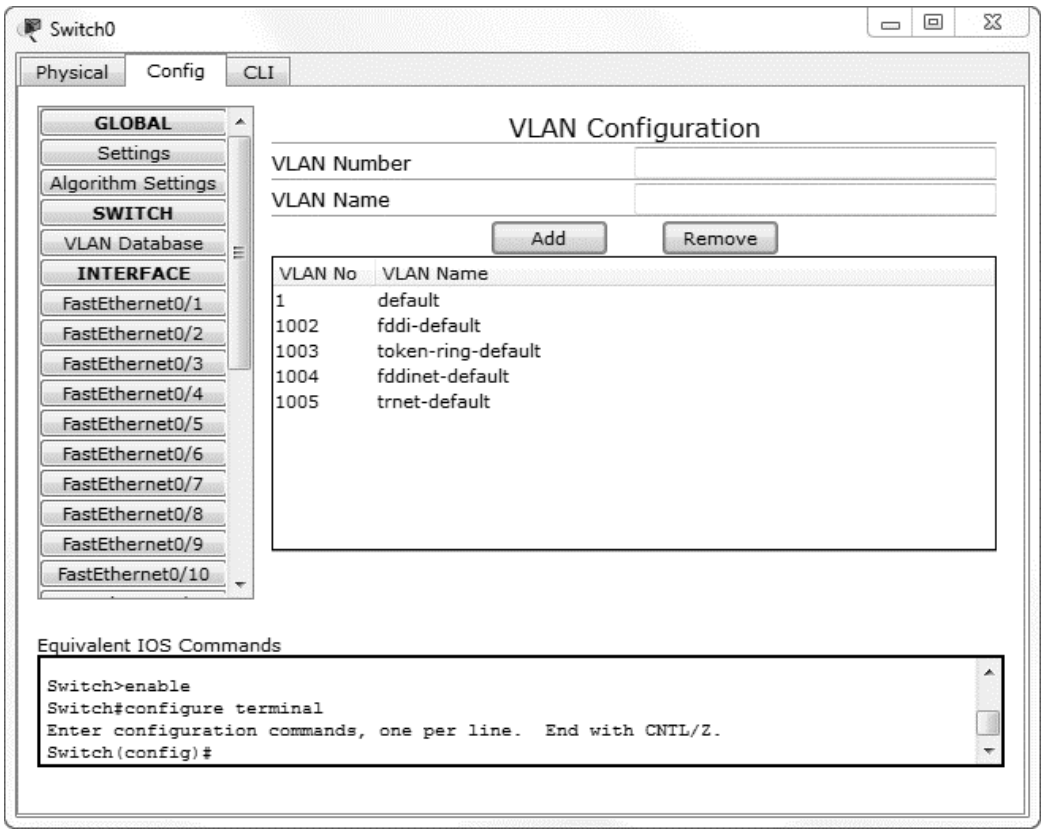

Abbildung 16

Die vorkonfigurierten Einträge können Sie an dieser Stelle ignorieren. Tragen Sie 3 VLAN – Netze in die Liste ein. Nutzen Sie dazu der Übersichtlichkeit wegen die Nummerierungen 10, 20 und 30. Die Namen der VLANs können sie selbst wählen. Den Eintrag fügen Sie mit einem Einfachklick auf *Add* hinzu. Begeben Sie sich in das Menü des Anschlusses *FastEthernet0* (dieser sollte mit *PC0* verbunden sein). Setzen Sie den VLAN – Modus auf *Access* und wählen Sie in der nebenstehenden Liste Ihr erstes angelegtes VLAN (10). Heben Sie sämtliche Auswahlen der anderen VLANS auf (Abbildung 17).

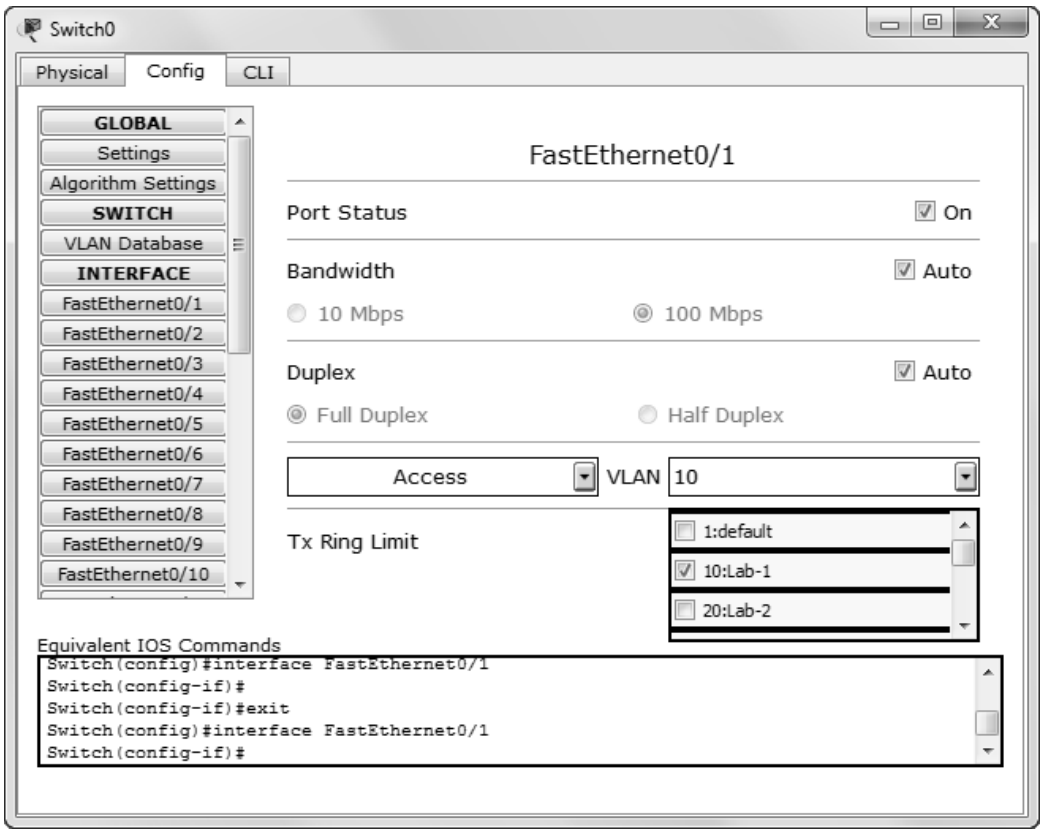

Abbildung 17

Wiederholen Sie diese Schritte für PC1 und das jeweils andere Computerpaar, welches Sie im gleichen VLAN geplant haben (nach Abbildung 14 *PC6* und *PC7*). Im Anschluss daran konfigurieren Sie für die zwei anderen Computerpaare die zwei anderen angelegten VLANs (nach Abbildung 14 *PC2 / PC3 – PC8 / PC9 VLAN 2*, *PC4 / PC5 – PC10 / PC11 VLAN 3*). Nach diesem Schritt ist Ihr einfaches VLAN konfiguriert und kann getestet werden. Wechseln Sie dazu in den Simulationsmodus und stellen Sie den Protokollfilter auf ICMP. Um die Funktionsweise des VLANS zu verstehen, senden Sie einige Simple PDUs zwischen den einzelnen VLANS hin und her. Verfolgen Sie dazu die einzelnen Pakete und machen Sie sich ein Bild von dem stattfindenden Datenverkehr. Wie sie sehen, ist eine Übertragung nur zwischen Geräten innerhalb eines VLANs möglich, was den Verwendungszweck dieser Technologie demonstriert. Um *Trunking* mit in die Umgebung einzubeziehen, löschen Sie zunächst sämtliche Szenarien und wechseln zurück in den Echtzeitmodus. Platzieren Sie einen weiteren Switch neben dem ersten und verbinden Sie die Geräte untereinander. Trennen Sie ebenfalls jeweils ein Computerpaar vom ersten Switch und schließen Sie die insgesamt 3 Gerätepaare an den neu platzierten Switch an (Abbildung 18).

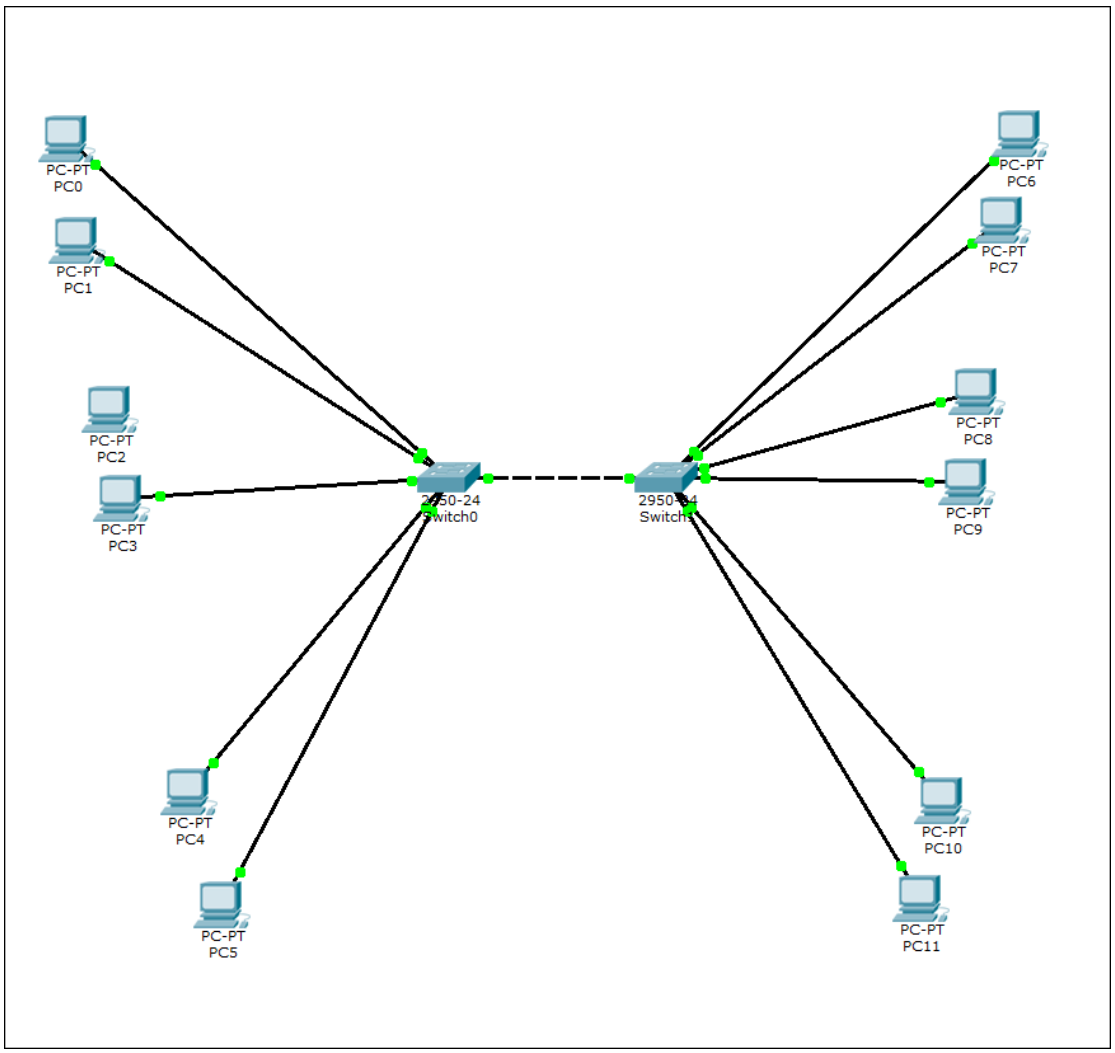

Abbildung 18

Richten Sie *Switch1* mit der Konfiguration von *Switch0* ein. Achten Sie dabei darauf, dass VLAN – Nummern und – Namen übereinstimmen. Begeben Sie sich nacheinander in die Konfigurationsfester der beiden Switches und rufen Sie jeweils die Ports auf, über welche die Geräte miteinander verbunden sind. Wechseln Sie den VLAN – Modus auf *Trunk* und setzen Sie die Häkchen in der nebenstehenden Liste bei allen 3 angelegten VLANs (Abbildung 19).

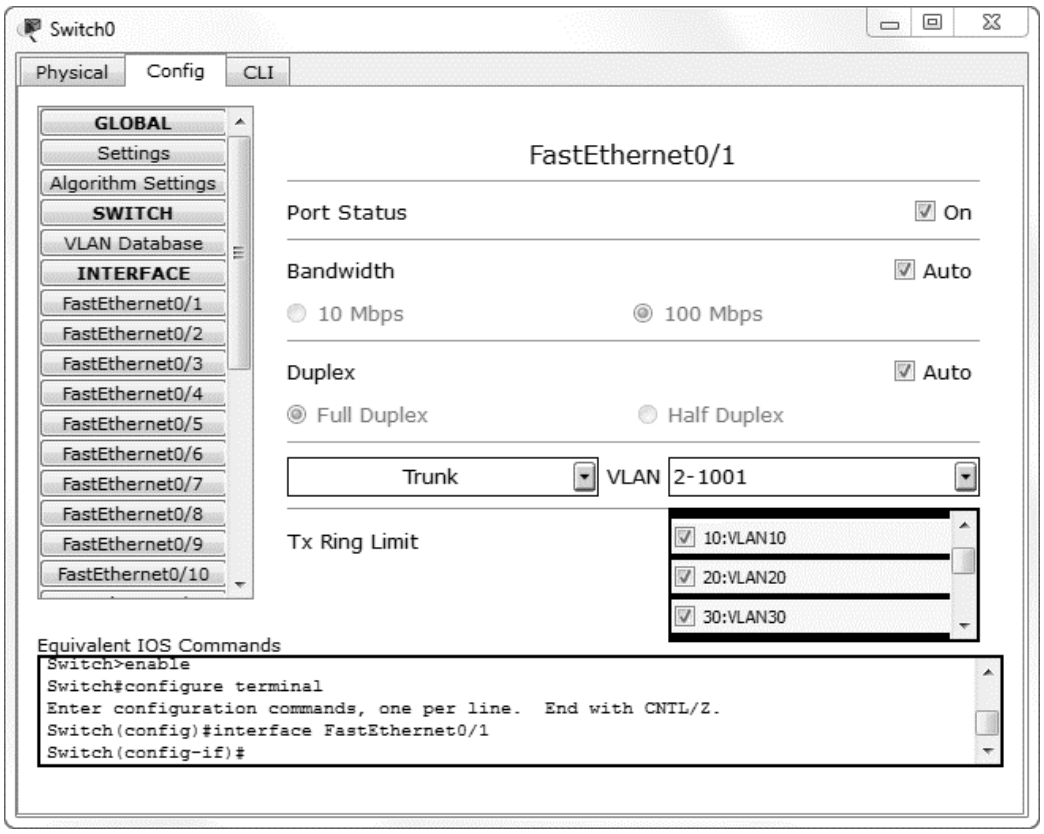

Abbildung 19

Dies bedeutet, dass der Trunk alle verwendeten VLANs verbindet und den Switches zugänglich macht. Richten Sie die Access – Ports am neuen Switch für alle PCs ein, welche an diesen angeschlossen sind (nach Abbildung 17 *PC6*, *PC7*, *PC8*, *PC9*, *PC10*, *PC11*) und weisen Sie diesen wieder die entsprechenden VLANs zu. Um die VLANs inklusive *Trunking* zu analysieren, wechseln Sie wieder in den Simulationsmodus und senden Sie eine einfache PDU von *PC0* an *PC6* (*VLAN10*). Verfolgen Sie den Transportweg des Pakets via *Capture / Forward*, bis dieses am ersten Switch eintrifft. Führen Sie einen Einfachklick auf das Briefsymbol aus, um die Detailansicht der Übermittlung aufzurufen. Wechseln Sie in *Layer 2* der *Out Layers* – Spalte (Abbildung 20).

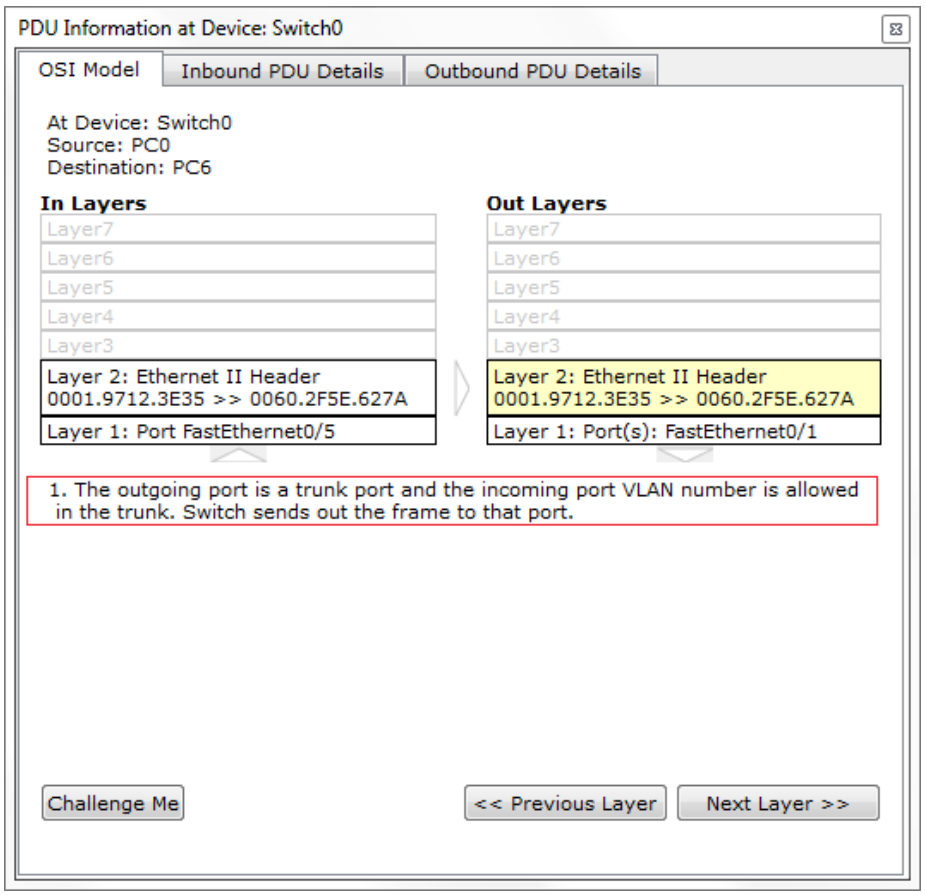

Abbildung 20

Hier sehen Sie, dass der Switch das Paket über den Trunk an den anderen Switch weiterleitet (vgl. Kommunikation über VLANs innerhalb eines Gebäudes auf mehreren Etagen). Durch die vorangegangenen Einstellungen erkennt der Switch, dass das eingehende Paket innerhalb eines VLANs versendet wird, welches auf dem Trunk zugelassen ist. Die Kommunikation kann fehlerfrei stattfinden.

Aufgabe 3: Einrichten und Konfiguration einer serverseitigen Firewall

Zum Einsatz kommende Hardware:

2 Generic PCs (Standard PC)

2 2950 – 24 Switches (Standard 24 – Port Switch)

1 1841 – Router (Standard Router)

1 Generic Server (Standard Server, Dienste: HTTP, DNS, FTP)

Ziel dieser Aufgabe ist es, eine, auf Seite des Servers installierte Firewall in ein überschaubares Netzwerk zu implementieren, um so die Arbeitsweise dieser Technologie zu analysieren. Die Kriterien der Firewall soll sich an den Protokollen ICMP, TCP und UDP orientieren. Dazu werden verschiedene Dienste im Netzwerk zuerst implementiert, um anschließend die Firewall zu konfigurieren und zu testen. Ebenfalls soll der Zusammenhang zwischen verschiedenen Protokollen und Diensten in der Netzwerktechnik mit dieser Aufgabe verdeutlicht werden. Platzieren Sie zu Beginn zwei PCs, den Switch, den Router und den Server auf der Arbeitsfläche. Verbinden Sie die PCs mit dem Switch und schließen Sie diesen an den Router an. Den zweiten Ethernet – Anschluss des Routers benutzen Sie zur Verbindung mit dem Server. Rufen Sie die IP Konfiguration des Servers auf. Vergeben Sie die IP Adresse *10.10.10.1* an den Server und nutzen Sie die vorgeschlagene Subnetzmaske. Schließen Sie vorerst das Konfigurationsfenster des Servers und begeben Sie sich in das IP Einstellungsfenster der PCs. Nutzen Sie für die IP Konfiguration *192.x.x.x* Adressen. Tragen Sie im Feld DNS Server die IP Adresse des Servers ein, da dieser später als DNS – Server fungieren wird. Schließen Sie die Konfigurationsfenster wieder. Wenden Sie sich dem Routing zu und ermöglichen Sie eine Kommunikation zwischen Clients (PCs) und Server (siehe auch *Versuch 2, Aufgabe 4*). Nach Abschluss der Konfiguration testen Sie die Kommunikation zwischen PCs und Server mittels *Simple PDU*. Funktioniert diese einwandfrei, wenden Sie sich erneut dem Server zu. Legen Sie im DNS – Menü des Servers zu Testzwecken einen Eintrag fest und schalten Sie den DNS Service auf *On* (Abbildung 21).

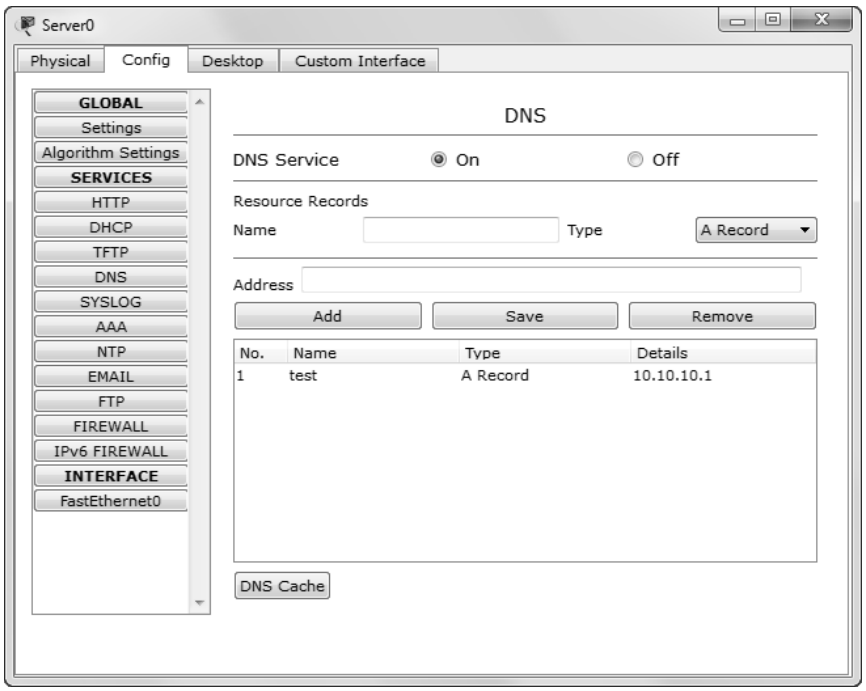

Abbildung 21

Vergewissern Sie sich, dass die Dienste HTTP und FTP aktiviert sind. Sind diese Einstellungen vollständig, kann mit der Konfiguration der Firewall begonnen werden. Navigieren Sie dazu in das entsprechende Menü über die Schaltfläche *FIREWALL* (Abbildung 22).

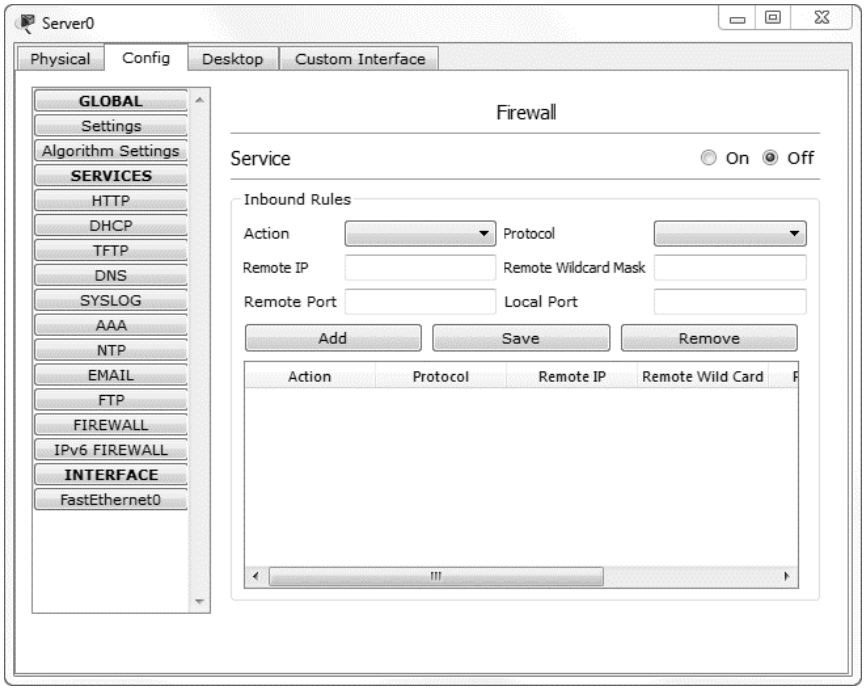

Abbildung 22

Zuerst soll eine Richtlinie für ICMP festgelegt werden. Es soll erreicht werden, dass eben jene Anfragen von der Firewall blockiert werden und somit keine Kommunikation über dieses Protokoll stattfinden kann. Wählen Sie entsprechend unter *Action* die Option *Deny*. Stellen Sie die *Protocol* – Schaltfläche auf *ICMP*. Im Feld *Remote IP* tragen Sie *192.0.0.0* ein, da sämtliche Anfragen aus diesem Netz geblockt werden sollen. Die zugehörige *Remote Wildcard Mask* lautet hier *0.255.255.255*. Für *Remote Port* und *Local Port* müssen Sie hier keine Einstellungen vornehmen. Fügen Sie den Eintrag mit einem Einfachklick auf *Add* hinzu. Die Richtlinie für ICMP Anfragen ist damit abgeschlossen. Weiterhin sollen noch 3 weitere Einträge hinzugefügt werden, welche die Protokolle TCP und UDP betreffen. Nehmen Sie diese Einstellungen mit Hilfe der nachfolgenden Tabellen vor.

Richtlinie für FTP

Action	*Deny*	Protocol	*TCP*
Remote IP	*192.0.0.0*	Remote Wildcard Mask	*0.255.255.255*
Remote Port	*any*	Local Port	*21*[7]

Richtlinie für HTTP

Action	*Allow*	Protocol	*TCP*
Remote IP	*192.0.0.0*	Remote Wildcard Mask	*0.255.255.255*
Remote Port	*any*	Local Port	*80*[8]

Richtline für DNS

Action	*Allow*	Protocol	*UDP*
Remote IP	*192.0.0.0*	Remote Wildcard Mask	*0.255.255.255*
Remote Port	*any*	Local Port	*53*[9]

[7] Port 21 – Standardisierter Port für FTP – Kontrollen
[8] Port 80 – Standardisierter Port für HTTP – Requests
[9] Port 53 – Standardisierter Port für DNS

Aktivieren Sie den Dienst, indem Sie die Schaltfläche *On* aktivieren. Mit diesen Einstellungen werden jetzt Anfragen aus dem 192.x.x.x - Netz blockiert, welche ICMP nutzen. Ebenfalls abgelehnt werden TCP – Anfragen auf Port 21, also FTP – Kontrollen. Zugelassen hingegen sind HTTP – Requests und Anfragen, die DNS benutzen. In den nächsten Schritten soll ein genauerer Blick auf diese Funktionsweise geworfen werden. Wechseln Sie in den *Simulationsmodus* und ändern sie den *Event List Filter* auf *ICMP*. Senden Sie eine *Simple PDU* von einem der beiden PCs an den Server und verfolgen Sie mit Capture / Forward den Übertragungsweg des Pakets. Sobald dieses den Server erreicht, wird es verworfen (Abbildung 23).

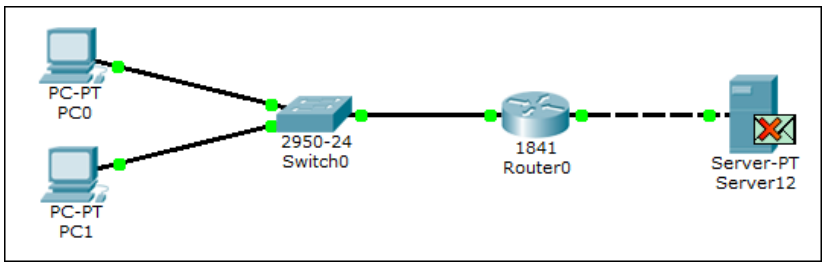

Abbildung 23

Führen Sie einen Einfachklick auf das Briefsymbol aus, um einen detaillierteren Einblick über die Übertragung zu erhalten. Schicht 1 und Schicht 2 arbeitet hier normal (Abbildung 24 und Abbildung 25).

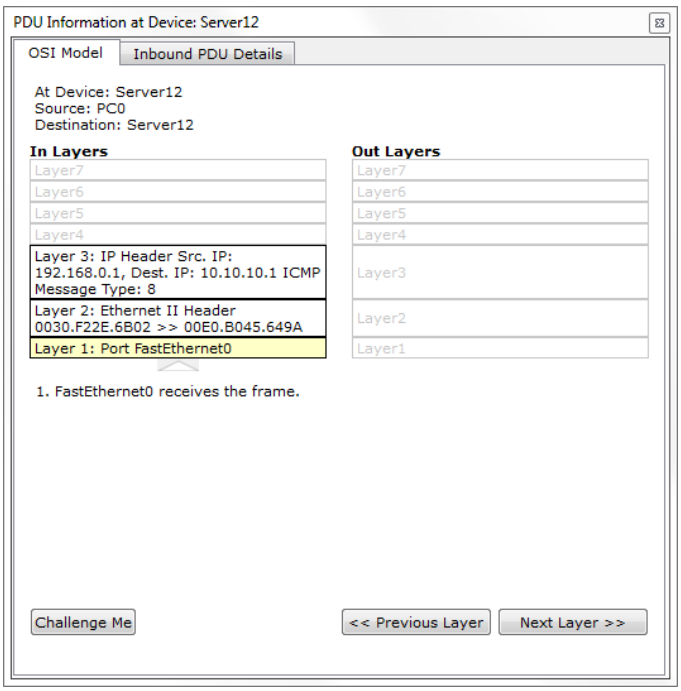

Abbildung 24

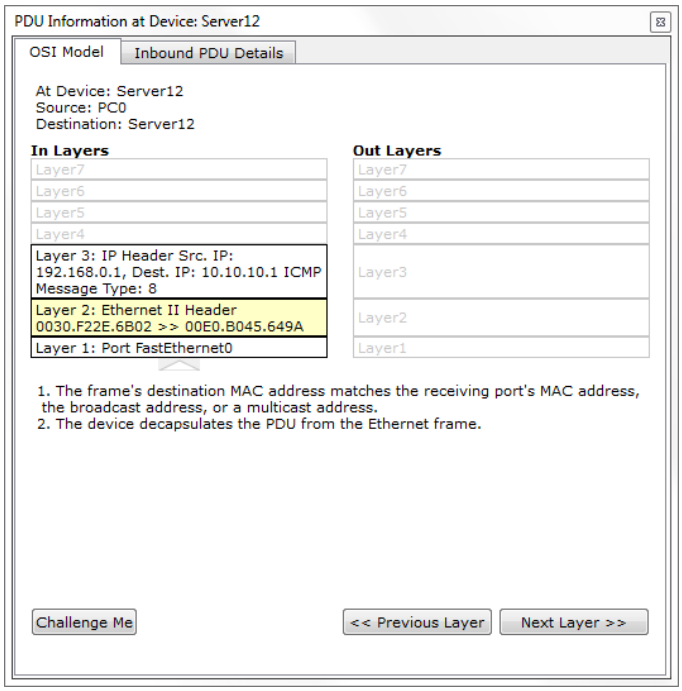

Abbildung 25

Da sich die konfigurierte Richtlinie auf ICMP Pakete beschränkt und keine Portbeschränkungen nennt, arbeitet diese als Paketfilter auf Schicht 3 des OSI – Referenzmodells. Per Einfachklick auf *Layer 3* rufen Sie die Informationen zur Paketübermittlung auf, welche auf Schicht 3 stattfinden. Sie erkennen, dass die Firewall des empfangenden Gerätes (hier: Server) erkannt wird und das

übertragene Paket mit der festgelegten Konfiguration abgleicht. Das Paket weist Übereinstimmungen mit den Ablehnungskriterien der Firewall auf und wird damit verworfen (Abbildung 26).

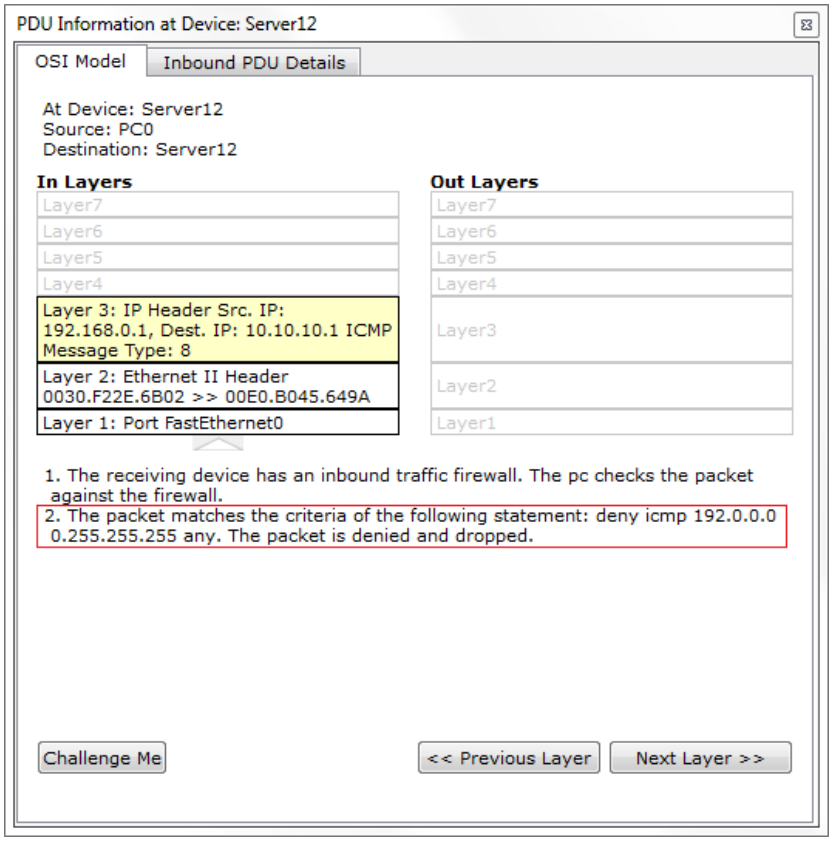

Abbildung 26

Um eine nächste Übertragung zu verfolgen, löschen Sie zunächst die zuletzt durchgeführte Übermittlung mit einem Einfachklick auf *Delete* im Szenario – Manager. Bei der nächsten Sendung soll es sich um eine FTP – Anfrage handeln. Stellen Sie also den Event Filter auf TCP, da für den Transport von FTP – Paketen dieses Protokoll verwendet wird. Öffnen Sie die Kommandozeile eines PCs via *Desktop / Command Prompt*. Geben Sie

ftp 10.10.10.1

in diese ein und schicken Sie den Befehl durch Betätigen der Enter – Taste ab. Es erscheint ein Briefsymbol am sendenden PC auf der Arbeitsfläche (Abbildung 27).

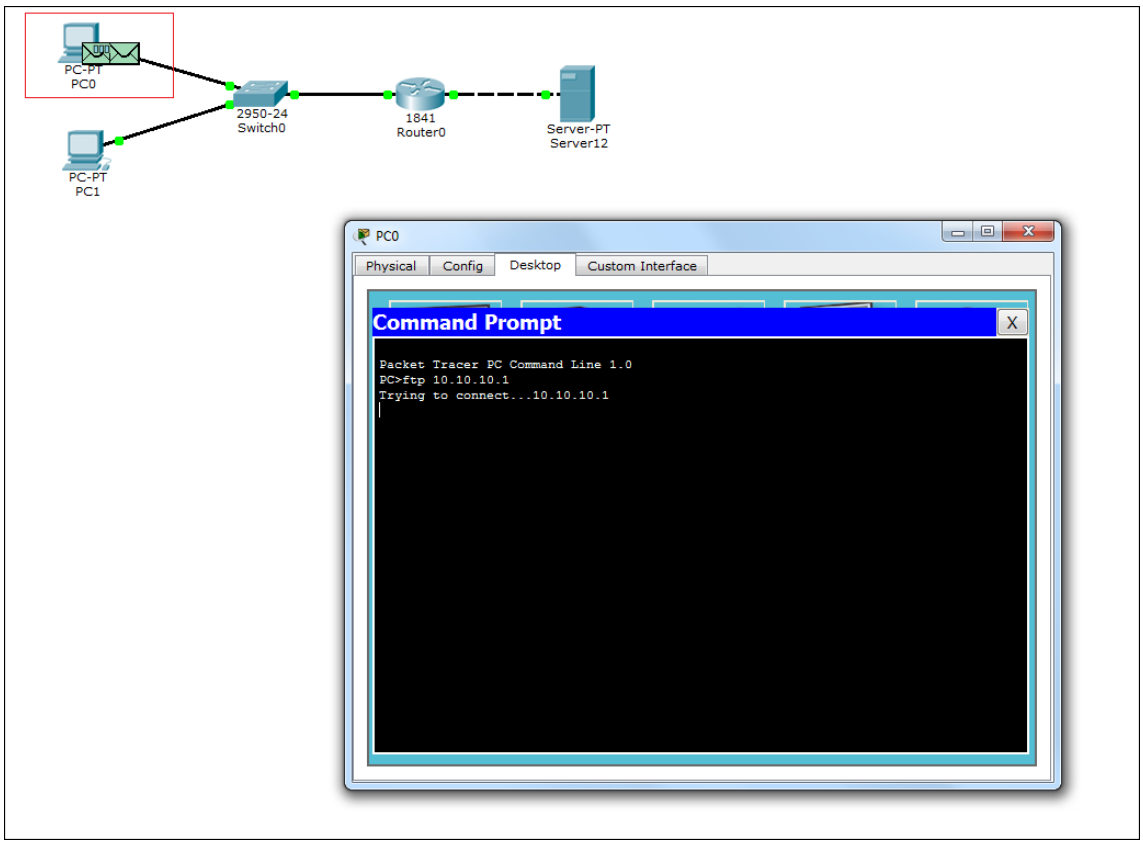

Abbildung 27

Per wiederholtem Klick auf *Capture / Forward* können Sie den Weg des Pakets erneut verfolgen. Sobald das Paket den Server erreicht hat, führen Sie einen Einfachklick auf das Briefsymbol aus. Unter Layer 3 wird Ihnen, wie schon bei der vorherigen Paketübertragung, angezeigt, dass dieses Paket ebenfalls die Ausschlusskriterien der Firewall erfüllt und somit verworfen wird. Im nächsten Schritt soll demonstriert werden, wie die Firewall zugelassene Pakete passieren lässt und eine Übertragung ermöglicht. Schließen Sie zuerst die Kommandozeile und entfernen Sie das eben durchgeführte Szenario wieder. Fügen Sie *DNS* dem *Event List Filter* hinzu. Begeben Sie sich anschließend zurück in die Desktopumgebung eines PCs und rufen Sie den Web Browser auf. In die Adresszeile geben Sie den Namen ein, welchen Sie in der DNS Konfiguration am Server festgelegt haben. Mit einem Einfachklick auf Go schicken Sie die Anfrage ab. Wieder erscheint das Briefsymbol am verwendeten PC. Per *Capture / Forward* können Sie den Weg des Pakets beobachten. Rufen Sie die Detailansicht erneut auf, sobald das Paket den Server erreicht. Layer 3 gibt Ihnen erneut Auskunft, wie die gesendete Einheit

behandelt wird. In diesem Fall erfüllt dieses die Zulassungskriterien der Firewall und wird weiter bearbeitet (Abbildung 28).

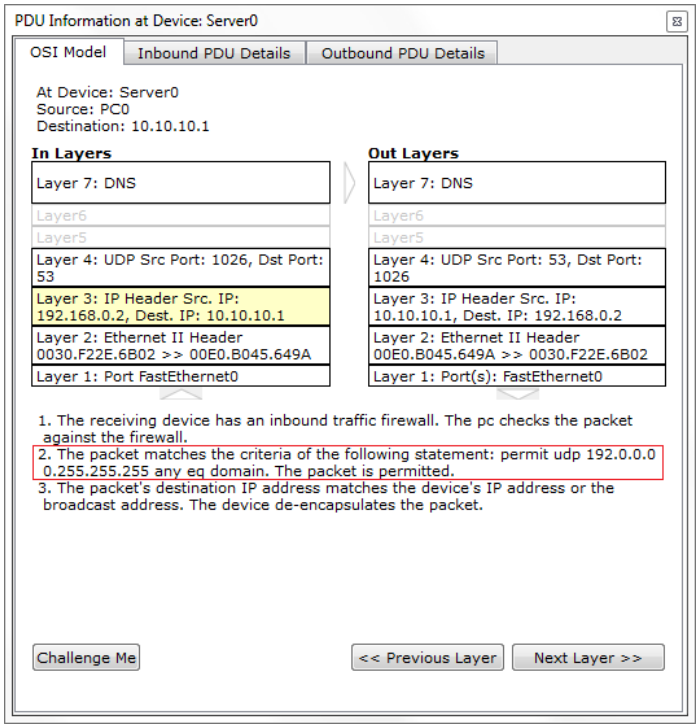

Abbildung 28

Diese Ansicht ermöglicht ebenfalls einen sehr guten Einblick in die Arbeitsweisen des DNS – Dienstes, in Hinblick auf das OSI – Modell. Mit einem Einfachklick auf *Auto Capture / Play* setzen Sie die komplette Kommunikation, ausgelöst durch den DNS – Request im Browser, fort und können diese verfolgen. Hier kann beispielsweise die Übersetzung des DNS – Namen in die zugehörige IP – Adresse eingesehen und beobachtet werden, welche Übertragungen hier stattfinden, bis letztendlich ein Ergebnis beim Client ankommt. Abschließend können Sie die Firewall nach Ihren Wünschen konfigurieren und verschiedene Szenarien testen.

Aufgabe 4: Simulation der IP – Übersetzung via NAT

Zum Einsatz kommende Hardware:

2 Generic PCs (Standard PC)

1 2950 – 24 Switch (Standard 24 – Port Switch)

2 Generic Router (Standard Router)

1 Generic Server (Standard Server)

In der Praxis ist die eigentliche IP Adresse eines Gerätes heutzutage nur noch selten die direkte Kontaktadresse für Kommunikationsanfragen von außen (Beispiel Webserver). Stattdessen werden sämtliche privat nutzbare Adressen in eine öffentliche IP – Adresse übersetzt, über welche sämtliche Anfragen dann erfolgen. Dies führt dazu, dass IP – Adressen von verschiedenen Clients mehrfach verwendet werden können (da sie logisch nur über eine öffentliche IP – Adresse kommunizieren) und somit die Verteilung der IPv4 – Adressen verlangsamt wird. Die grundlegende Funktionsweise dieser Technologie soll in dieser Aufgabe mit einem Packet Tracer Szenario demonstriert werden. Platzieren Sie zuerst zwei handelsübliche Computer, welche über einen Switch mit dem Generic Router verbunden sind, auf der Arbeitsfläche. Zusätzlich setzen Sie einen Server und verbinden Sie ihn mit einem weiteren Generic Router. Verbinden Sie beide Router mit einem  Serial DCE – Kabel. Das Netzwerk kann nun konfiguriert werden (Abbildung 29).

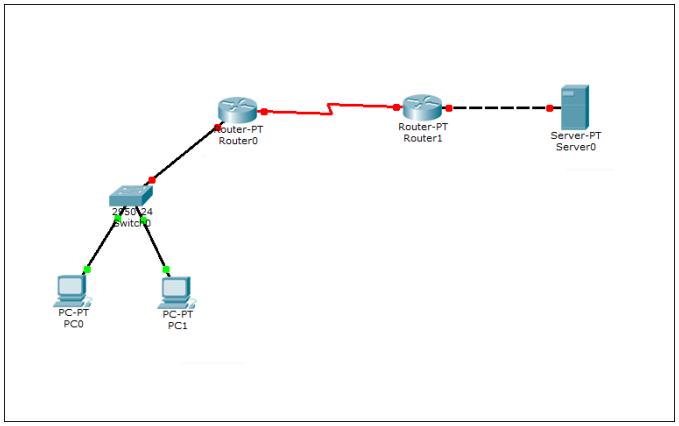

Abbildung 29

Zuerst vergeben Sie statische IP – Adressen an die Endgeräte. Nutzen Sie für die PCs 192.168.1.x – Adressen. Konfigurieren Sie dementsprechend am *FastEthernet* – Port von *Router0* eine Adresse als Gateway für dieses Netz und aktivieren Sie den Port. Tragen Sie die Gateway – Einstellungen in die IP – Konfigurationen der Computer ein. In einem nächsten Schritt konfigurieren Sie den Server und den dazugehörigen Router1. Nutzen Sie für den Server die IP 10.0.0.254. Dem dazugehörigen Routeranschluss geben Sie die IP 10.0.0.1. Tragen Sie diese ebenfalls als Gateway am Server ein. Abschließend vergeben Sie noch die öffentlichen IPs an die seriellen Ports der Router:

Router0 200.10.0.1

Router1 200.10.0.2

Die IP – Konfigurationen der Geräte ist jetzt abgeschlossen. Um eine Kommunikation zwischen Server und Clients zu ermöglichen, müssen Sie eine IP Route festlegen, die den Transport ermöglicht. Dies soll hier über eine die Default Route 0.0.0.0 0.0.0.0 erfolgen. Öffnen Sie dazu die Konsole von Router0 und begeben Sie sich in den globalen Konfigurationsmodus. Setzen Sie die Route und definieren Sie diese über den seriellen Anschluss mit dem Befehl

ip route 0.0.0.0 0.0.0.0 s2/0

Schließen Sie das Konfigurationsfenster von Router0 und wiederholen Sie diesen Schritt bei Router1. Nun kann eine Kommunikation zwischen Server und PCs stattfinden. Testen Sie dies, indem Sie eine Simple PDU von einem der beiden PCs an den Server senden (Echtzeitmodus). Öffnen Sie zu Demonstrationszwecken den Webbrowser von PC0 und geben Sie die IP des Servers in die Adresszeile ein (vergewissern Sie sich, dass der http Dienst am Server aktiviert ist). Es wird Ihnen die konfigurierte Website angezeigt. In der Praxis ist die direkte IP des Webservers jedoch nie bekannt. Der Request wird an ein Gerät (hier Router1) mit einer öffentlichen IP gesendet, welche diesen dann an den Server weiterleitet und die Antwort zurückleitet. Dabei wird dessen IP via NAT übersetzt, womit als Source – IP hier die öffentliche IP des Routers im IP Header des Pakets auftaucht. Dies soll nachfolgend demonstriert werden. Um eine Detailüberblick auf die Übertragung ohne NAT zu werfen, begeben Sie sich in den Simulationsmodus und stellen Sie den Event Filter auf ICMP. Schicken Sie erneut eine Simple PDU von PC0 an den

Server und verfolgen Sie die Übertragung mittels Capture / Forward bis das Paket Router1 erreicht. Öffnen Sie die Detailansicht per Einfachklick auf das Briefsymbol und rufen Sie die Inbound PDU Details auf (Abbildung 30).

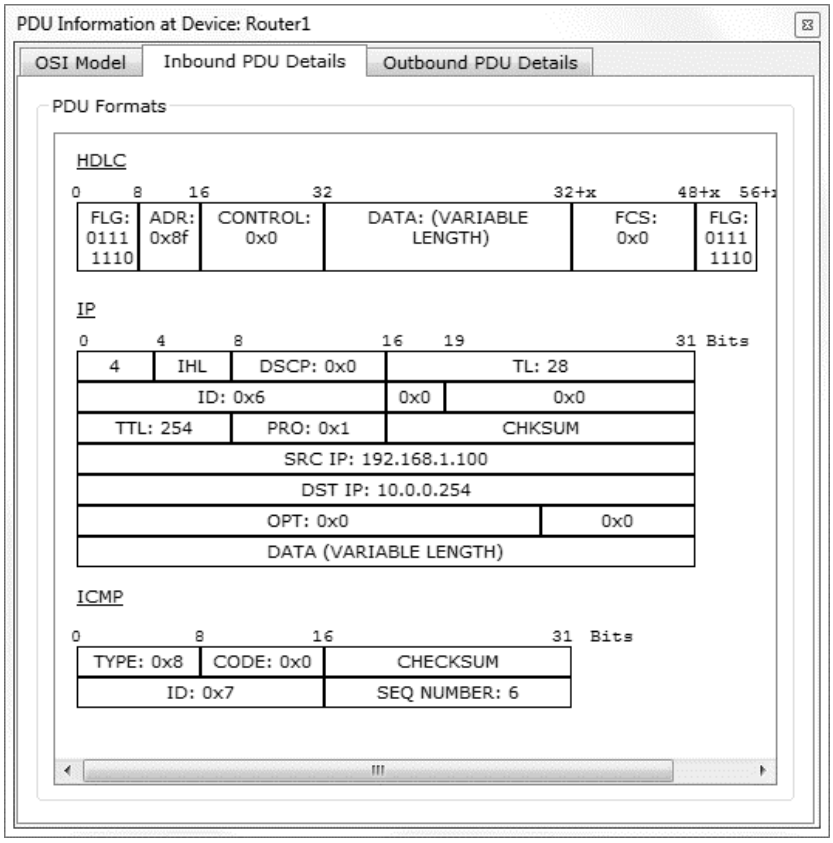

Abbildung 30

Wie zu erkennen, ist als Ziel – IP die direkte IP des Servers im Paket enthalten. Ebenso findet sich als Source IP die Adresse des sendenden Rechners. Löschen Sie das aktuelle Szenario und begeben Sie sich zurück in den Echtzeitmodus. Um NAT zu konfigurieren, begeben Sie sich in die Konsole des Serverrouters und rufen den globalen Konfigurationsmodus auf. Zunächst sollen alle Pakete, welche vom Server kommen, auf die öffentliche IP Adresse des Routers übersetzt werden. Dabei wird die Adresse des Servers auf die öffentliche Adresse des Routers gemappt. Dies geschieht über den Befehl

ip nat inside source static 10.0.0.254 200.10.0.2

Im nächsten Schritt muss dem Router mitgeteilt werden, welcher Port als Ein- bzw. als Ausgang für die NAT – Übersetzung verwendet werden soll. Begeben Sie sich per

interface fa0/0

in die Konfiguration des Ethernet – Ports, an den der Server angeschlossen ist und definieren Sie ihn via

ip nat inside

als Eingangsport. Verlassen Sie mit *exit* diesen Port und wechseln Sie mit

interface s2/0

zum seriellen Port. Legen Sie mit dem Befehl

ip nat outside

diesen Port als Ausgangsport für die Adressübersetzung fest. Durch zweimaliges Absenden des *exit* – Befehls und einmaliges Betätigen der Enter – Taste gelangen Sie zurück in den Standard Konfigurationsmodus des Routers. Speichern Sie Ihre Einstellungen mit dem Befehl

copy run start

und bestätigen Sie die nachfolgende Frage mit Enter (Abbildung 31).

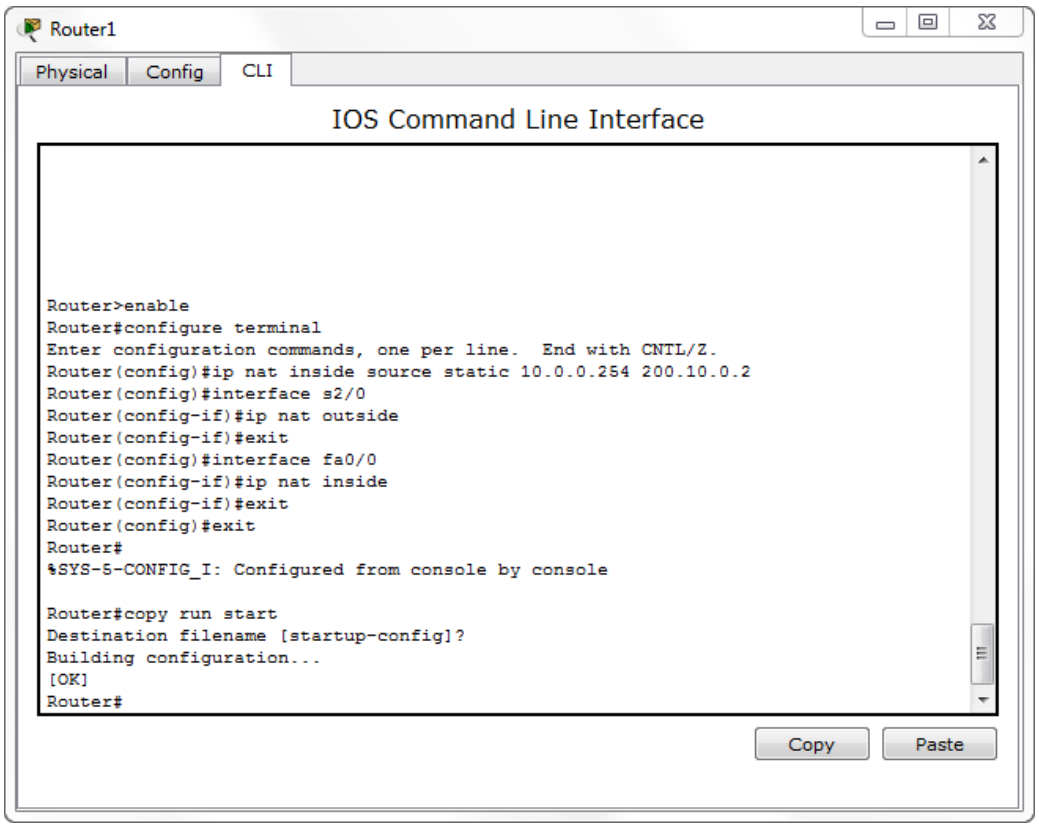

Abbildung 31

Schließen Sie die Konsole. Serverseitig ist die NAT Technologie an dieser Stelle implementiert. Dies können Sie überprüfen, indem Sie erneut den Webbrowser eines PCs aufrufen. Geben Sie die IP – Adresse des Servers ein, werden Sie kein Ergebnis erhalten. Benutzen Sie hierfür allerdings die Öffentliche IP – Adresse des Serverrouters, wird Ihnen die Website angezeigt. Im nächsten Schritt wird NAT auch in Router0 eingebunden. Öffnen Sie dazu die Konsole von Router0 und arbeiten Sie sich in den globalen Konfigurationsmodus vor. Zuerst wird hier eine Zugangsliste angelegt, welche es erlaubt, sämtliche Geräte des Netzes 192.168.1.x an diesem Router zu betreiben. So muss nicht jedes einzelne Gerät manuell am Router auf NAT konfiguriert werden. Diese Liste legen Sie mit dem Befehl

access-list 1 permit 192.168.1.0 0.0.0.255

an. Die verwendete Wildcard Maske steht hier für die umgekehrte Subnetzmaske. Mit dem nächsten Befehl

ip nat inside source list 1 interface s2/0 overload

kommt NAPT zum Einsatz, da alle Geräte, welcher zu List1 gehören, werden auf die öffentliche Adresse des seriellen Ports am Router übersetzt werden. Abschließend müssen Ein- und Ausgangsport definiert und die Einstellungen gespeichert werden. Gehen Sie dabei wie bei der Konfiguration des Serverrouters vor (achten Sie auf die korrekten Portbezeichnungen, an denen Sie die Geräte angeschlossen haben). Ist dies abgeschlossen können Sie das Konsolenfenster schließen und die NAT Konfiguration testen. Rufen Sie die Kommandozeile eines PCs auf und versuchen Sie, mittels *ping 10.0.0.254* den Server direkt zu erreichen. Da auf Grund der NAT – Übersetzung der Server so nicht mehr antwortet, wird keines der gesendeten Datenpakete erfolgreich übermittelt (Abbildung 32).

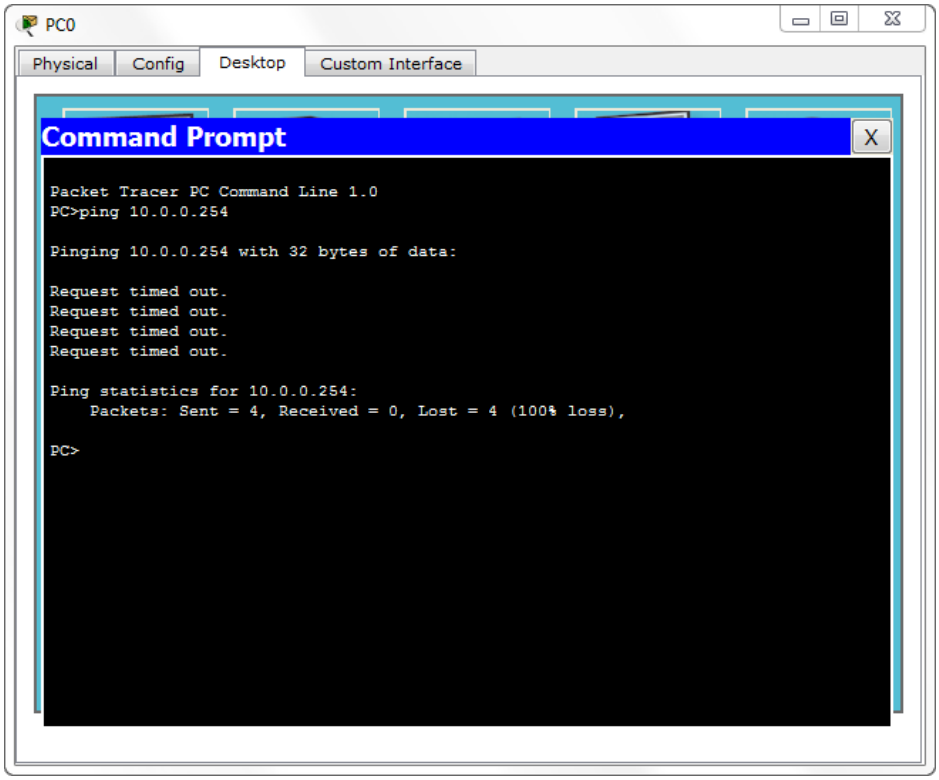

Abbildung 32

Wechseln Sie in den Simulationsmodus und starten Sie eine Übertragung mittels Simple PDU von PC0 an den Serverrouter. Verfolgen Sie das Paket, bis dieses bei Router0 angekommen ist und öffnen Sie die Detailansicht der Übertragung. Rufen Sie nacheinander die Inbound PDU Details und die Outbound PDU Details auf (Abbildung 33 und Abbildung 34).

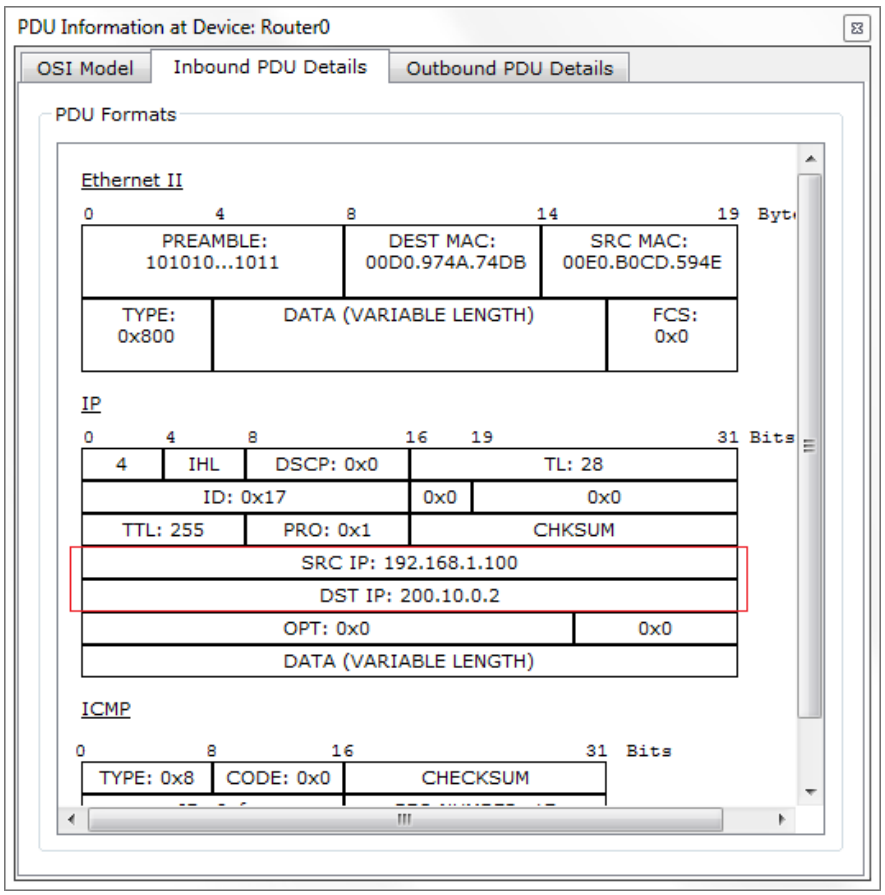

Abbildung 33

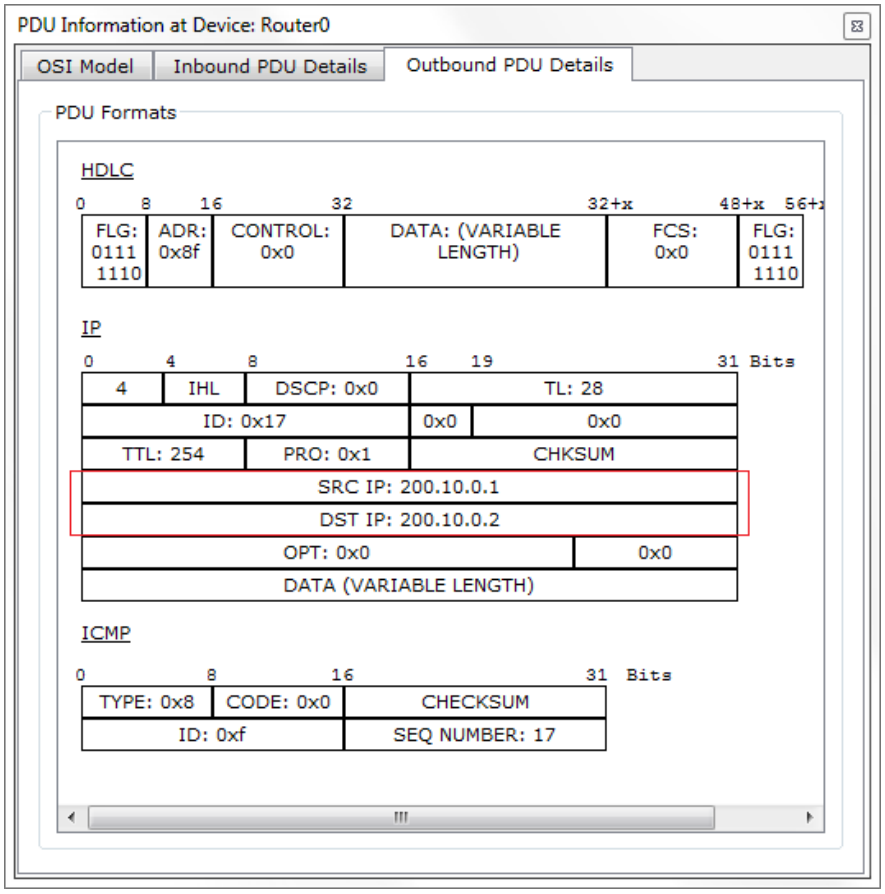

Abbildung 34

Hier wird deutlich, dass die Source IP des Rechners nur im IP Header des Pakets vorhanden ist, bis dieses den Router erreicht. Dieser übersetzt diese Adresse via NAT, wie in den Outbound PDU Details erkennbar ist. Beobachten Sie den weiteren Verlauf des Pakets. Obwohl Sie die PDU an Router1 geschickt haben, wird das Paket an den Server weitergeleitet. Rufen Sie die Detailansicht der Übertragung auf, wenn diese den Server erreicht hat und navigieren Sie die in die Outbound Details (Abbildung 35).

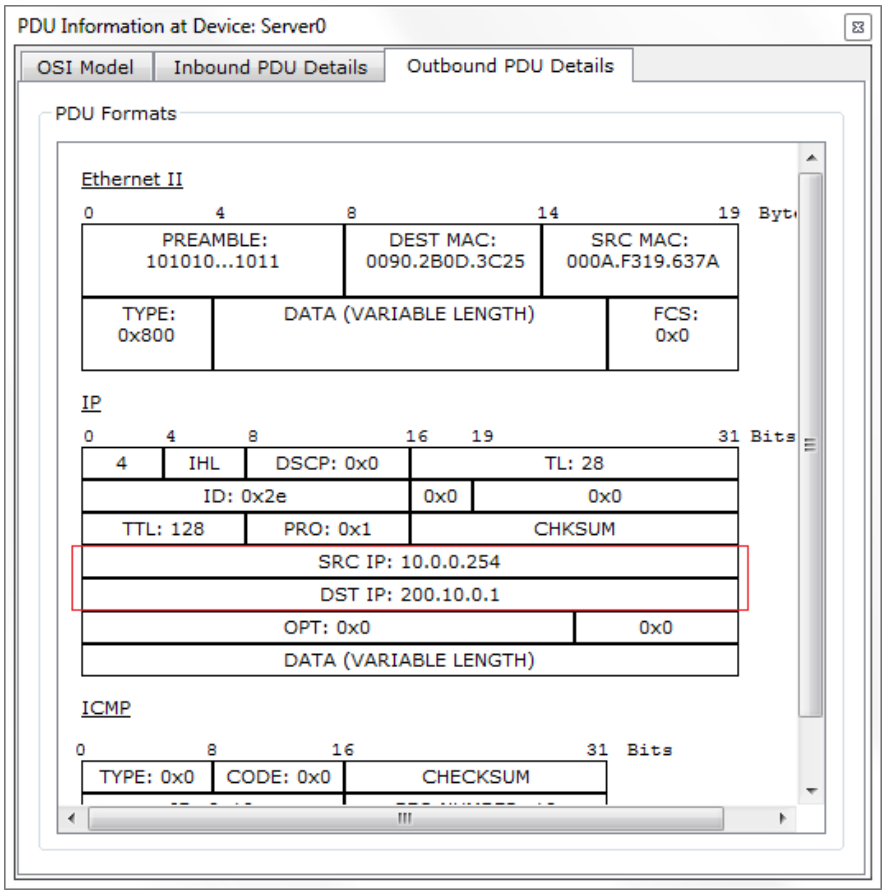

Abbildung 35

Der Server schickt dieses Paket an die öffentliche IP des Routers, da ihm durch die NAT – Übersetzung die ursprüngliche Herkunft des Paketes nicht bekannt ist. Das Paket wird in den nächsten Schritten über Router1 zurück an Router0 übermittelt, wo es die Ziel IP des sendenden PCs zurückerhält, damit dieser die Antwort entgegennehmen kann.

Aufgabe 5: Simulation eines IPv6 – basierenden Netzwerkes

Zum Einsatz kommende Hardware:

3 Generic PCs (Standard PC)

2 2950 – 24 Switches (Standard 24 – Port Switch)

1 1841 – Router (Standard Router)

Durch die NAT – Technologie kann die Verteilung und das damit verbundene Zuneigegehen der IPv4 Adressen deutlich gebremst werden. Jedoch bringt NAT auch Probleme mit sich (siehe auch Rubrik IPv6 – Adressierung, Vorlesungsskript Administration und Netzwerktechnik II), weshalb IPv6 als Nachfolge für IPv4 entwickelt wurde. Diese Aufgabe widmet sich der Simulierung eines einfachen privaten Netzwerkes, welches auf IPv6 – Adressierungen basiert (siehe auch Rubrik IPv6 – Adressierung, Vorlesungsskript Netzwerktechnik und Administration II). Mittels der Packet Tracer Software soll dieses Netzwerk aufgebaut werden und einige, in der Vorlesung behandelte Elemente simulieren. Arrangieren Sie zunächst alle benötigten Geräte auf der Arbeitsfläche. Es sollen insgesamt 3 PCs, ein Router, sowie zwei Switches zum Einsatz kommen. Der erste und zweite Computer sind über einen Switch an den Anschluss *FastEthernet0/0* des Routers angeschlossen. Über das weitere Interface *FastEthernet0/1* des Routers ist der dritte Computer über einen zweiten Switch verbunden (Abbildung 36).

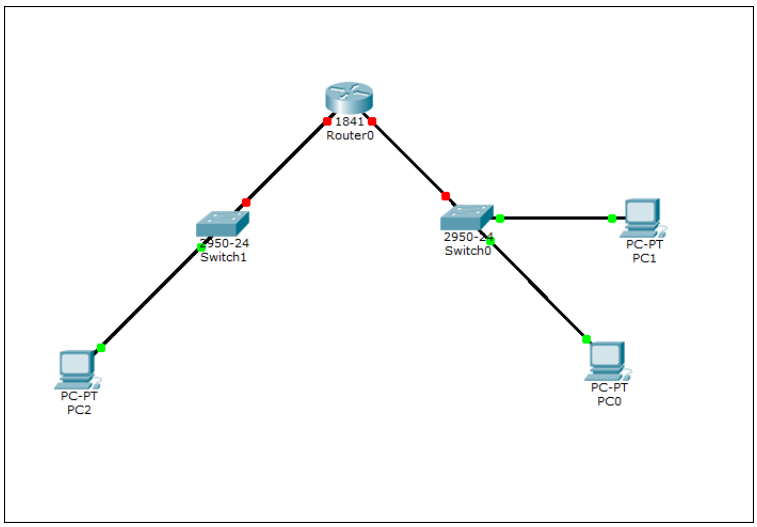

Abbildung 36

In einem nächsten Schritt soll der Router für die Arbeit mit IPv6 vorbereitet und die Link – Local Adressen der beiden verbundenen Routerinterfaces konfiguriert werden. Normalerweise werden diese Adressen zwar beim Start eines Gerätes automatisch erzeugt, jedoch ist es zu Administrationszwecken von Vorteil, diese Einstellung (zumindest in diesem Größenumfang) manuell vorzunehmen. Begeben Sie sich dazu in die Konsole von Router0. Verschaffen Sie sich Zugang zum globalen Konfigurationsmodus. Aktivieren Sie das IPv6 – Routing mittels des Befehls

ipv6 unicast-routing

Der Router kann jetzt damit arbeiten. Nachfolgend soll die Link – Local Adresse von Interface *FastEthernet0/0* festgelegt werden. Diese soll *FE80::1* lauten (verkürzte Schreibweise). Begeben Sie sich per

interface fa0/0

in die Konfigurationsumgebung für diesen Anschluss. Mit Hilfe des Befehls

ipv6 address FE80::1 link-local

weisen Sie diese Adresse dem Port zu und definieren Sie gleichzeitig als Link – Local Adresse. Speichern Sie diese Konfiguration mit Hilfe der Eingabe

no shutdown

und betätigen nach der Bestätigung dieses Befehls erneut die Enter – Taste, um zurück in den Konfigurationsmodus zu gelangen.

Verlassen Sie per *exit* die Konfiguration dieses Anschlusses und wenden Sie sich via

interface fa0/1

dem anderen Port zu. Auf Grund der Funktionsweise von IPv6 und der rein lokalen Signifikanz der Link – Local Adresse kann der Port FastEthernet0/1 ebenfalls die Adresse FE80::1 erhalten. Weisen Sie diesem Anschluss ebenfalls diese Adresse zu und speichern Sie diese Konfiguration. Beide Anschlussknoten des Routers sollten grün gekennzeichnet sein. Jedoch kann noch keine Kommunikation zwischen den beiden Netzen stattfinden, da der Router, sowie die Endgeräte noch keine routingfähigen globalen Unicast – Adressen besitzen. Für die Konfiguration soll eine IPv6 Adresse verwendet werden, welche ein 64bit – Netzwerkpräfix besitzt. Für Netz 1 (Anschluss *FastEthernet0/0*) soll folgende Adresse verwendet werden:

2*001:00A1:AAAA:000A:0000:0000:0000:0001* (volle Schreibweise)

(Netzpräfix 2001:00A1:AAAA:000A)

2001:A1:AAAA:A::1 (verkürzte Schreibweise)

Hierbei handelt es sich bei 2001:A1:AAAA:A um den Netzwerkpräfix von Subnetz *A*. Äquivalent dazu, jedoch im Subnetz *B*, soll Port *FastEthernet0/1* folgende Adresse erhalten:

2*001:00A1:AAAA:000B:0000:0000:0000:0001* (volle Schreibweise)

(Netzpräfix 2001:00A1:AAAA:000B)

2001:A1:AAAA:B::1 (verkürzte Schreibweise)

Begeben Sie sich zurück in die Konsole des Routers. Rufen Sie den Konfigurationsmodus von Anschluss *FastEthernet0/0* auf und weisen Sie diesem mittels des Befehls

ipv6 address 2001:A1:AAAA:A::1/64

diese Adresse zu (mittels */64* wird mitgeteilt, dass 64 Bits der Adresse zum Netzpräfix zugehörig sind). Verlassen Sie mit *exit* das Interface FastEthernet0/0 und vergeben Sie an Netz 2 (Anschluss *FastEthernet0/1*) die Adresse des B – Subnetzes. Der Router ist nun konfiguriert und das Konsolenfenster kann geschlossen werden. Um zu überprüfen, ob die Endgeräte ihre eigenen IPv6 – Adressen beziehen, öffnen Sie die IP – Konfiguration eines PCs und schalten Sie in den IPv6 – Einstellungen von *Static* auf *Auto Config*. Sind alle Konfigurationsschritte erfolgreich durchgeführt worden, erzeugt das Gerät jetzt eine IPv6 – Adresse, basierend auf der MAC – Adresse des Netzwerkadapters. Ebenfalls wird das IPv6 – Gateway erkannt (Link – Local Adresse des Routerinterfaces) (Abbildung 37).

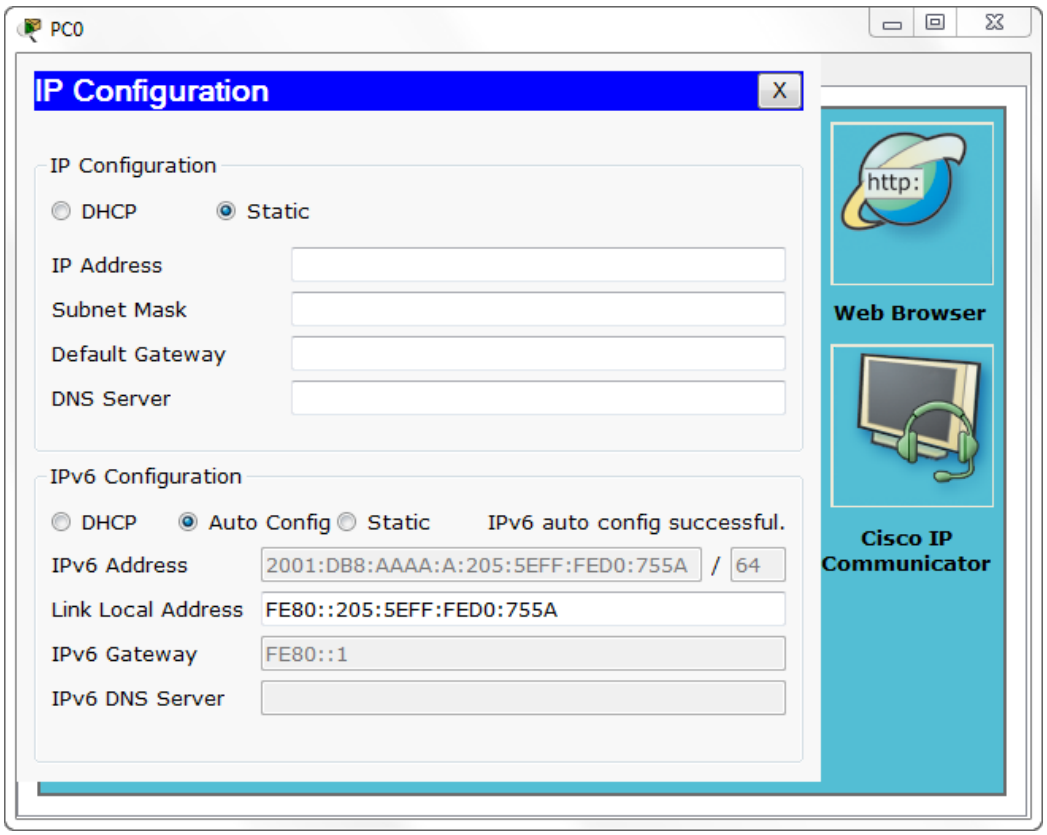

Abbildung 37

An diesem Beispiel sieht man, dass die Adresse im Subnetz A generiert. Wiederholen Sie diese Schritte bei den anderen PCs und achten Sie darauf, welche Adresse jener PC in Subnetz B generiert. Anschließend können Sie die Kommunikation zwischen den PCs untereinander analysieren. Senden Sie dazu zunächst im Echtzeitmodus mehrere einfache PDUs zwischen den Computern hin

und her, um die Mac – Adressenermittlung in der Detailansicht zu umgehen. Wechseln Sie in den Simulationsmodus und stellen Sie den Event Filter auf ICMPv6. Senden Sie eine Simple PDU von *PC0* an *PC2* und verfolgen Sie die Paketübermittlung schrittweise mittels *Capture / Forward*. Öffnen Sie die Detailansicht des Pakets, sobald dieses den Router erreicht und werfen Sie einen Blick auf die *Inbound Details* (also die am Router ankommenden Paketdetails) (Abbildung 38).

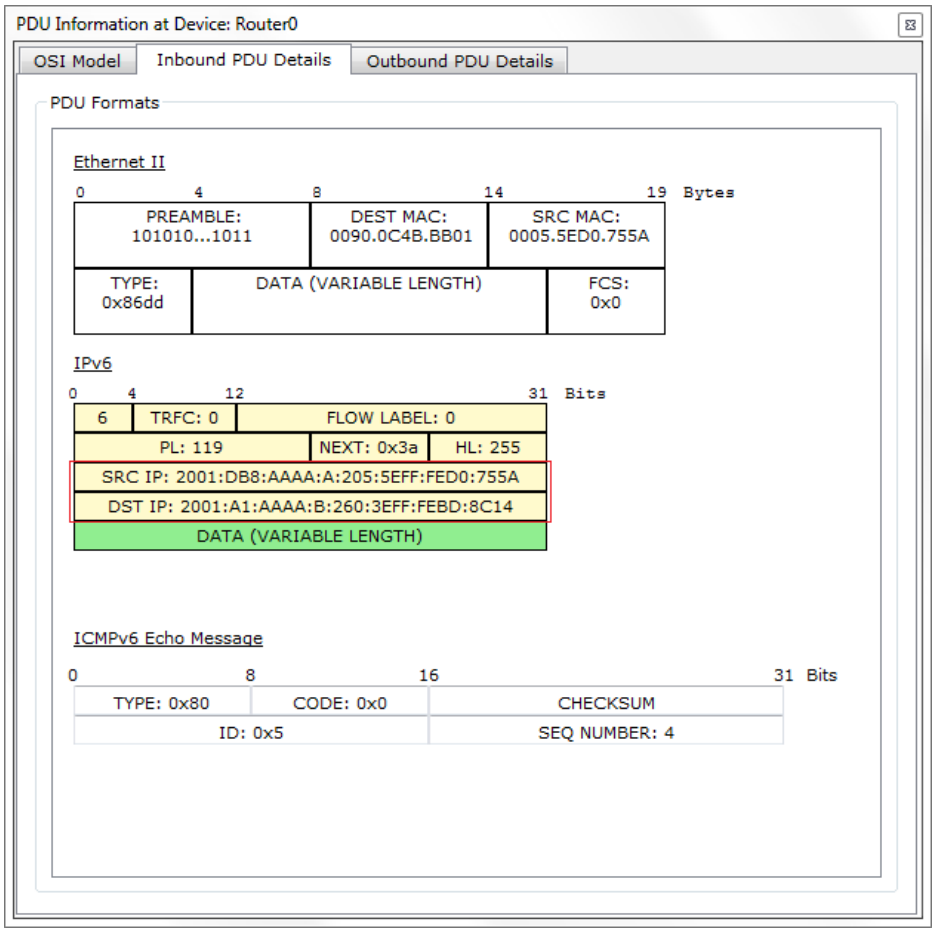

Abbildung 38

Hier deutlich zu erkennen, die für Source – und Destination IP aufgelisteten IPv6 – Adressen. Die erfolgreiche Übertragung des Pakets findet also komplett über IPv6 – Mechanismen statt und ohne die herkömmlichen IPv4 – Konfigurationen, wie Adresse oder Subnetzmaske.

Aufgaben zum Versuch

1. Von welcher Technologie stellt MAN eine Sonderform dar?

2. Was bedeutet VLAN und wozu dient es?

3. Auf welcher Schicht des OSI – Modells arbeiten paketfilterbasierende Firewalls?

4. Wie funktioniert NAT und wozu wird es verwendet? Welche Nachteile hat es?

5. Wo liegt der Unterschied zwischen IPv4 und IPv6 Adressierungen?

Versuch 4: Packet Tracer – Komplexversuch

Studiengänge	▪ Medientechnik
Ausbildungsziel	▪ Kennenlernen weiterer Cisco – Konsolenfunktionen ▪ Festigung des Verständnisses für Funktionsweisen von verschiedenen Technologien
Ausbildungsinhalte	▪ Einrichtung, Test und Betrachtung eines Komplexszenarios am Beispiel einer Internetverbindung unter Betrachtung der Technologien auf Anwender-, sowie auf Anbieterseite ▪ Weitere Beispiele zur Konsolenkonfiguration von Cisco Geräten
Hardware / Software	▪ 1 PC mit Virtual Box inklusive vorinstallierter Packet Tracer Software
Vorkenntnisse	▪ Versuch 1, Versuch 2, Versuch 3 ▪ Theoretische Grundlagen der Vorlesungsunterlagen Netzwerktechnik und Administration I & II

In diesem abschließenden Versuch sollen die erworbenen Kenntnisse aus der Vorlesung und den vorangegangenen Praktika gefestigt und selbstständig angewandt werden. Dabei soll im Rahmen eines Komplexbeispiels mit Hilfe der Packet Tracer Software eine funktionsfähige Umgebung erstellt werden, welche einen üblich heimischen Internetzugang inklusive aller dazugehörigen Technologien simuliert. Dieser Komplexversuch ist unter einer Aufgabe in mehrere Abschnitte geteilt, die es schrittweise zu bearbeiten gilt. Sämtliche, schon behandelte Konfigurationen (beispielsweise IP Zuweisungen, Geräteeinstellungen) sollen selbstständig durchgeführt werden. Unbekannte Sachverhalte werden wie in den vorangegangenen Versuchen erläutert.

Aufgabe: Simulation einer Internetanbindung inklusive Anwender und Server

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)	
Generic Laptop (Standard Laptop, als Drahtlosgerät)	
Smart Device (z.B. Smartphone, als Drahtlosgerät)	
2950 – 24 Switch (Standard 24 – Port Switch)	
1841 – Router (als Heim- und ISP – Router)	
Generic Access Point (Anbindung von Drahtlosgeräten)	
DSL Modem (Anbindung an das Internet)	
Generic Cloud (Provideranbindung)	
Generic Server (Web-, Mail-, DNS – Server)	
Phone (Telefonkabel zur Anbindung des DSL Modems)	

Abschnitt 1: Konfiguration eines Heimnetzes

In dieser Aufgabe soll eine komplette Anbindung an das Internet simuliert werden, wie Sie sie von zuhause kennen. Dabei sollen sämtliche Technologien, welche dabei zum Einsatz kommen und in der Vorlesung bzw. den ersten 3 Versuchen behandelt worden sind, selbstständig implementiert und konfiguriert werden. Zuerst soll die Heimumgebung ordnungsgemäß konfiguriert und sich anschließend der Providerseite gewidmet werden. Dazu platzieren Sie zunächst einen *1841 – Router*, zwei *PCs*, einen *Standard 24 – Port Switch*, einen *Standard Access Point*, sowie ein *DSL Modem* auf der Arbeitsfläche. Zusätzlich fügen Sie einen *Laptop* und ein *Smart Device* hinzu, welche als Drahtlosgeräte zum Einsatz kommen sollen. Verkabeln Sie die platzierten Geräte wie gewohnt miteinander (der Access Point wird ebenfalls an den Switch angeschlossen). Zum besseren Verständnis können Sie Switch, Router und DSL Modem lokal zusammenfassen, da diese 3 Geräte in den meisten Haushalten als ein kombiniertes Gerät vorkommen. Dabei fungiert das DSL Modem als Anbindung nach außen. (Abbildung 1).

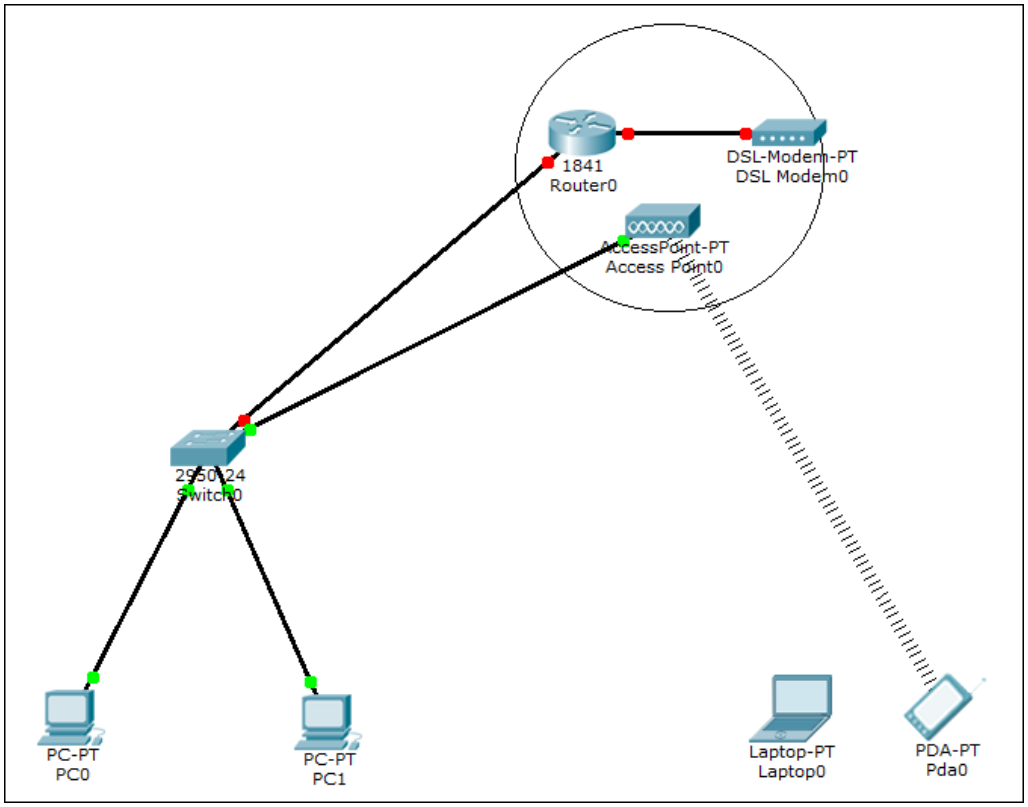

Abbildung 1

Wie Sie sehen, hat sich das PDA bereits mit dem Access Point verbunden. Dem Laptop muss zunächst noch manuell ein WLAN Modul hinzugefügt werden. Öffnen Sie dazu die Konfigurationsoberfläche des Laptops und verweilen Sie in dem geöffneten Reiter *Physical*. Im *Physical Device View* schalten Sie den Laptop zunächst ab, indem Sie einen Einfachklick auf den Powerbutton ausführen. (Abbildung 2).

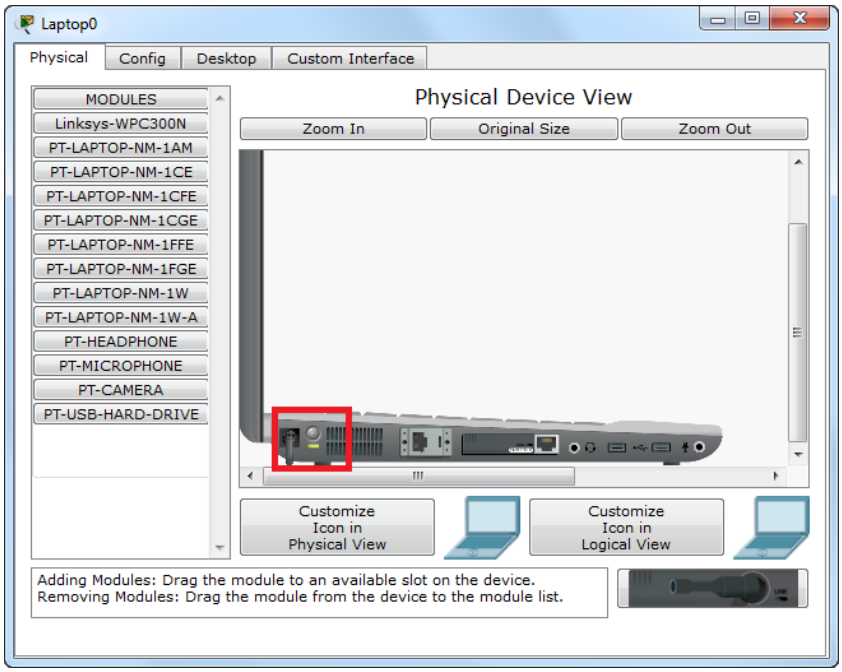

Abbildung 2

Anschließend entfernen Sie das bereits verbaute Modul, indem Sie dieses per *Drag and Drop* in das Feld in der unteren rechten Ecke führen. Wählen Sie aus der nebenstehenden List das *Linksys-WPC300N* – Modul aus und platzieren Sie es ebenfalls per Drag and Drop in dem eben frei gewordenen Steckplatz am Gerät (Abbildung 3).

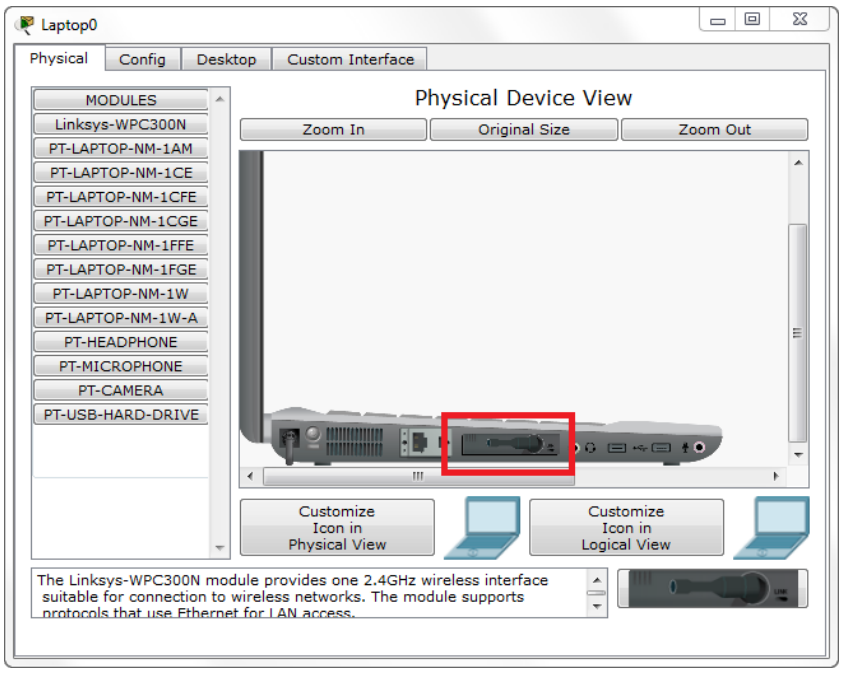

Abbildung 3

Nachdem Sie das Modul hinzugefügt haben, schalten Sie den Laptop wieder ein. Dieser verbindet sich automatisch mit dem Access Point. Von einer Drahtloskonfiguration (Verschlüsselungsverfahren, Passwort etc.) soll hier abgesehen werden. In einem nächsten Schritt soll die IP Vergabe via DHCP konfiguriert werden. Die Rolle des DHCP – Servers übernimmt hier der Router. Im Anwenderbereich des Netzwerkes sollen IPs eines üblichen Heimnetzwerkes zum Einsatz kommen, wobei der Router als Gateway nach innen eine entsprechende IP Adresse erhalten soll. Um die DHCP – Konfiguration durchzuführen, öffnen Sie die Konsole des Routers, begeben sich in den globalen Konfigurationsmodus und konfigurieren Sie den Router auf DHCP. Denken Sie dabei auch an die Zuweisung des Gateways. Schließen Sie mit *end* die Konfiguration ab und verlassen Sie die Konsole. Installieren Sie das Gateway am entsprechenden Port. Stellen Sie anschließend alle Endgeräte auf den IP – Bezug per DHCP um und stellen Sie sicher, dass die DHCP Vergabe fehlerfrei funktioniert. Im Anschluss daran überlegen Sie sich einen Weg, um die Kommunikationsfähigkeit aller Endgeräte im Heimnetz untereinander zu überprüfen. Ist eine Kommunikation gewährleistet, bleibt noch die Konfiguration des Gateways nach außen mit einer öffentlichen IP – Adresse. Ist diese erfolgt, ist das Heimnetz einsatzbereit.

Abschnitt 2: Konfiguration eines zweiten Heimnetzes

Richten Sie ein zweites Anwendernetz mit beliebig vielen Komponenten ein.

Abschnitt 3: Konfiguration des Servernetzes und Anforderungsumsetzung

In einem nächsten Schritt soll die serverseitige Konfiguration vorgenommen werden. Folgende Sachverhalte sollen umgesetzt werden:

1. Von den Endgeräten beider Heimnetze solle die Website www.hs-mittweida.de durch Eingabe der Domain über den Web Browser erreichbar sein.

2. Ein Endgerät aus Heimnetz 1 soll via Email (xxx@hs-mittweida.de) mit einem Endgerät aus Heimnetz 2 kommunizieren können.

3. Nach außen sollen alle Endgeräte in den Heimnetzen unter derselben, für den betreffenden Anschluss öffentlich gültigen IP Adresse auftreten.

Konfigurieren Sie eine Serverumgebung unter Verwendung geeigneter Technologien, um diese Forderungen zu erfüllen. Denken Sie auch an eine geeignete IP – Konfiguration. Ist die serverseitige Konfiguration abgeschlossen, binden Sie diese Umgebung an einen *1841 – Router* an, welcher hier als *ISP*[1] – *Router* fungieren soll. Konfigurieren Sie die beiden verwendeten *FastEthernet* – Anschlüsse dieses Routers so, dass eine Verbindung zwischen Anbieter und Nutzer prinzipiell möglich wäre. Überlegen Sie sich dabei geeignete IP Konfigurationen, welche diese Kommunikation ermöglicht. Haben Sie alle Anforderungen an das Servernetz umgesetzt, ist dessen Konfiguration abgeschlossen. Nehmen Sie alle weiteren Einstellungen vor, um die Heimnetze an die geforderten Gegebenheiten anzupassen.

Abschnitt 4: Verknüpfung von Servernetz und Heimnetz

Im Folgenden soll eine Verbindung zwischen Endbenutzer und Serviceanbieter hergestellt werden und damit das Internet sozusagen nachgebildet werden.

[1] Als ISP (Internet Service Provider) wird ein Anbieter bezeichnet, welcher bestimmte Dienste und Inhalte bereitstellt, welche für die Funktion des Internets erforderlich sind. Als ISP – Router wird hier der Router zur Anbindung an einen solchen Anbieter bezeichnet.

Platzieren Sie dazu eine 

Cloud – PT, welche Sie im Gerätemanager unter *WAN Emulation* finden (Abbildung 4).

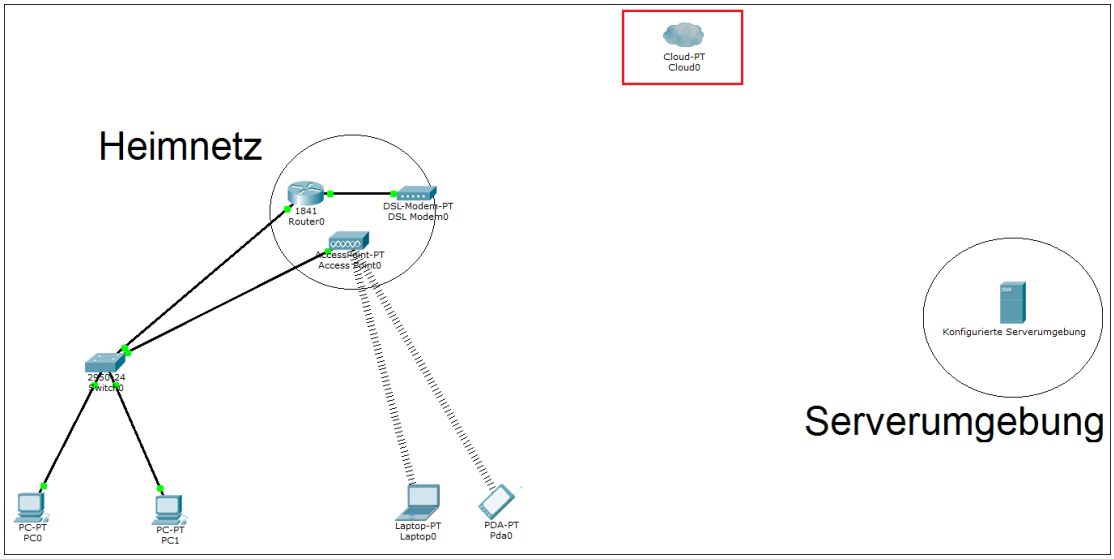

Abbildung 4

Wählen Sie im Connections – Menü ein  Standard – Telefonkabel und verbinden Sie das DSL Modem von Heimnetz 1 mit dem Anschluss *Modem4* der Cloud. Den *Ethernet6* – Anschluss der Cloud verbinden Sie mit dem ISP – Router, um die Serverseite anzubinden (Abbildung 5).

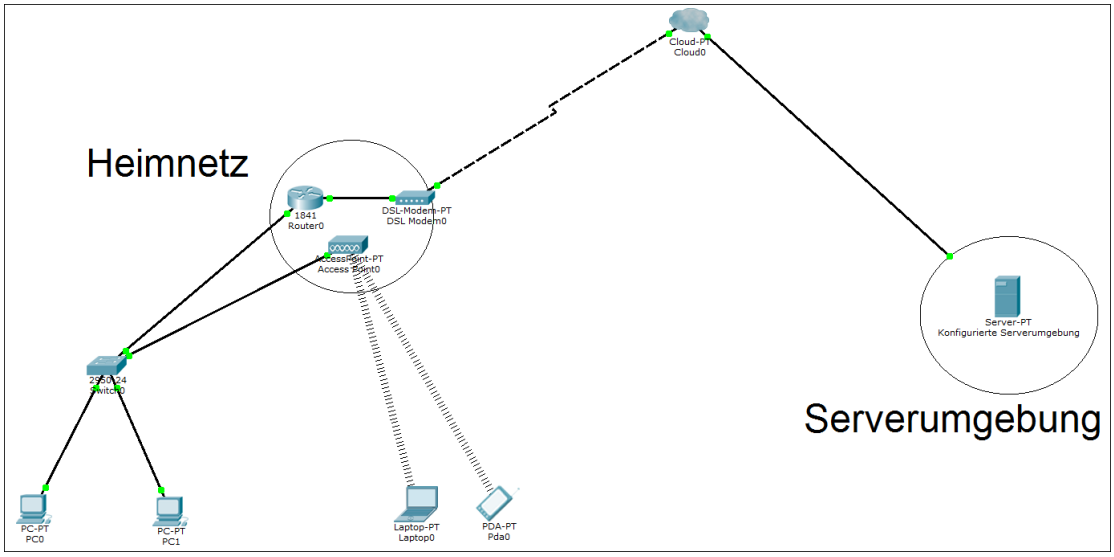

Abbildung 5

In einem nächsten Schritt muss nun der Übertragungsweg in der Cloud festgelegt werden, damit das DSL Modem im Heimnetz den ISP bei entsprechenden Anfragen

kontaktieren kann. Dazu begeben Sie sich via Einfachklick auf die Cloud in deren Konfigurationsoberfläche und navigieren Sie im Reiter *Config* in das Untermenü *DSL*. Dort legen Sie jetzt fest, dass zwischen dem Anschluss *Modem4* des Heim – DSL Modems und dem *Ethernet6* Port eine Übertragung stattfinden soll und fügen Sie den Eintrag per *Add* hinzu (Abbildung 6).

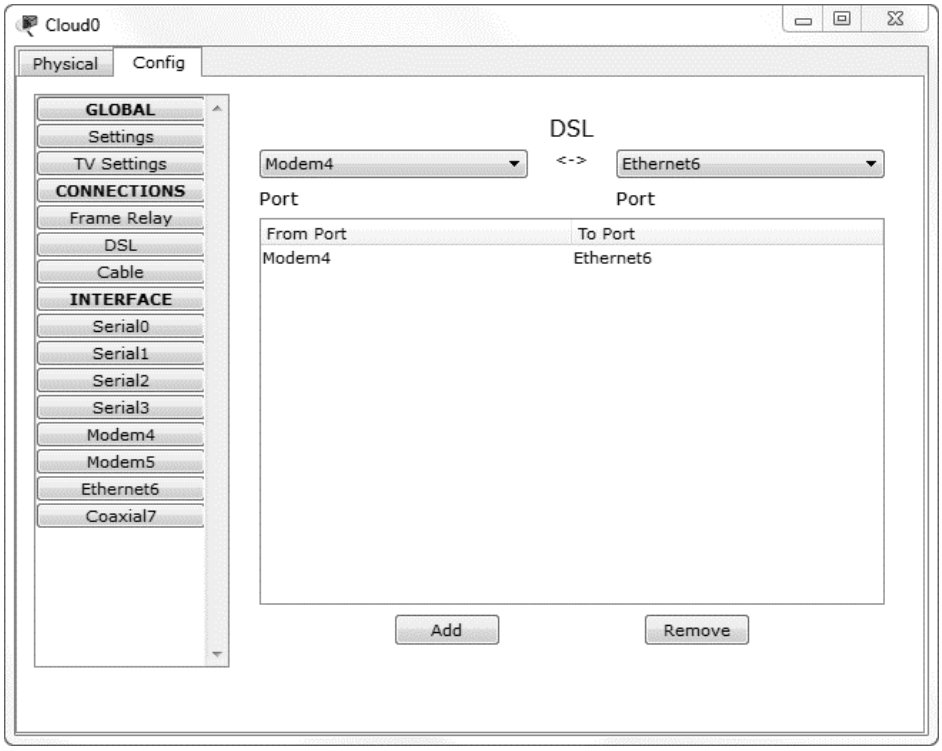

Abbildung 6

Schließen Sie das Einstellungsfenster. Verbinden Sie in einem weiteren Schritt Heimnetz 2 ebenfalls nach diesem Schema. Um eine Kommunikation zwischen ISP und den Routern des Heimnetzes zu gewährleisten, müssen Sie in deren Einstellungen noch IP – Routen festlegen. Dies geschieht hier unter der Schaltfläche *RIP*[2]. Hier müssen jeweils die Netze des anliegenden Netzwerkes eingetragen werden, um eine Übermittlung zu gewährleisten (also das Netz des Heimnetzwerkes, sowie die Adressierungen des öffentlichen Routernetzes, Abbildung 7).

[2] RIP (Routing Information Protokoll) ist ein Protokoll, welches zur automatischen Erstellung von Routingtabellen genutzt wird.

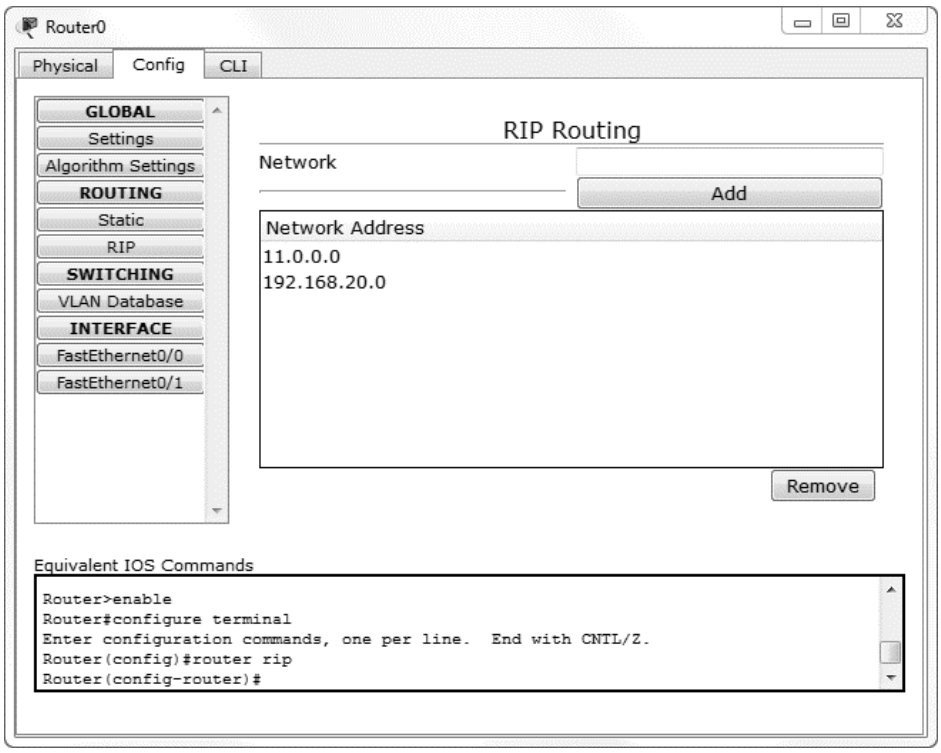

Abbildung 7

Nehmen Sie alle weiteren Einstellungen vor, die für eine funktionierende Kommunikation zwischen Anwender und Anbieter benötigt werden und testen Sie ihre Konfigurationen auf Funktion sämtlicher gestellter Anforderungen an das Szenario.

Abschnitt 5: Allgemeine Informationen zum Verständnis

Abschließend soll die folgende Grafik veranschaulichen, wie die verwendeten Netzwerkkomponenten in einem realen Szenario geografisch zuzuordnen sind, um Ihnen ein besseres Verständnis über die eigentliche Beschaffenheit des Internets zu vermitteln (Abbildung 8).

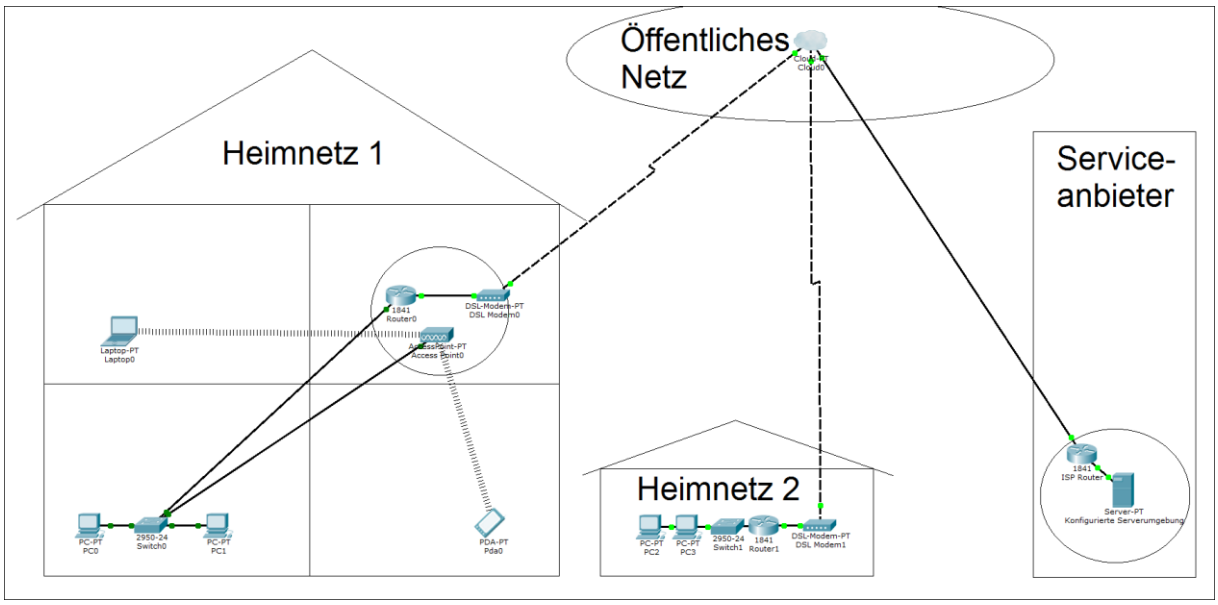

Abbildung 8

Das öffentliche Netz umfasst hier sämtliche Einrichtungen, welche die Haushalte mit den verschiedenen Anbietern verbinden, also Vermittlungsstellen, *DSLAMs*[3] usw.

[3] DSLAMs (Digital Subscriber Line Access Multiplexer) sind Komponenten der DSL – Infrastruktur. Haushaltsanschlussleitungen laufen hier zusammen. Also sogenannte *Outdoor – DSLAMs* kommen sie beispielsweise in Form der bekannten grauen Kästen vor, wie sie sich häufig in Orten finden lassen.

Anlagen, Teil 2, Geräteliste

Router (Tab. A.1)

1841

Cisco-Router mit zwei integrierten FastEthernet-Ports, einem USB-Anschluss und zwei Slots zur Erweiterung mit Interfacekarten.

1941

Cisco-Router mit zwei integrierten GigabitEthernet-Ports, zwei USB-Anschlüssen, sowie zwei Slots zur Erweiterung mit Interfacekarten.

2620XM

Cisco-Router mit einem integrierten FastEthernet-Port, sowie zwei Slots zur Erweiterung mit Interfacekarten. Zusätzlich ist ein Modulslot vorhanden.

2621XM

Cisco-Router mit zwei integrierten FastEthernet-Ports, sowie zwei Slots zur Erweiterung mit Interfacekarten. Zusätzlich ist ein Modulslot vorhanden.

2811

Cisco-Router mit zwei integrierten FastEthernet-Portts, zwei USB-Anschlüssen, sowie zwei Slots zur Erweiterung mit Interfacekarten. Zusätzlich ist ein Modulslot vorhanden.

2901

Cisco-Router mit zwei integrierten GigabitEthernet-Ports, zwei USB-Anschlüssen, sowie 4 Slots zur Erweiterung mit Interfacekarten.

2911

Cisco-Router mit 3 integrierten GigabitEthernet-Ports, zwei USB-Anschlüssen, sowie 4 Slots zur Erweiterung mit Interfacekarten.

Generic - Router

Selbst konfigurierbarer Router mit 10 Slots zur Erweiterung mit Interfacekarten.

Switches (Tab. A.2)

2950 – 24

Cisco-Switch mit 24 integrierten FastEthernet-Ports.

2950T – 24

Cisco-Switch mit 24 integrierten FastEthernet-Ports, sowie zwei GigabitEthernet-Ports.

2960 – 24TT

Cisco-Switch mit 24 integrierten FastEthernet-Ports, sowie zwei GigabitEthernet-Ports.

3560 – 24PS Multilayer

Cisco-Switch mit 24 integrierten FastEthernet-Ports, sowie zwei GigabitEthernet-Ports.

Bridge

Cisco-Bridge mit zwei Slots zur Erweiterung mit Interfacekarten.

Generic - Switch

Selbst konfigurierbarer Switch mit 10 Slots zur Erweiterung mit Interfacekarten.

Kabellose Geräte (Tab. A.3)

Verschiedene AccessPoints	
Cisco-Access Point mit einem integrierten FastEthernet-Port.	
Linksys Wireless Router (inklusive GUI)	
Linksys Wireless Router mit 4 integrierten FastEthernet-Ports (automatisch konfiguriert).	

Endgeräte (Tab. A.4)

PC 

Handelsüblicher PC, mit verschiedenen Interfaces ausstattbar und integrierter Desktopoberfläche.

Laptop 

Handelsüblicher Laptop, mit verschiedenen Interfaces ausstattbar und integrierter Desktopoberfläche.

Server 

Handelsüblicher Server mit einem integriertem FastEthernet-Port, sowie einen Slot zur Erweiterung mit Interfacekarten. Grafische Benutzeroberfläche.

Drucker 

Drucker mit integriertem FastEthernet-Port, welcher durch weitere Interfaces ersetzt werden kann.

IP – Telefon 

IP-Telefon mit simulierter grafischer Oberfläche. Zu Testzwecken.

VoIP – Gerät

VoIP-Gerät mit integriertem FastEthernet-Port.

Telefon

Analoges Telefon mit Telefonanschluss. Zu Testzwecken.

TV

Fernsehgerät mit TV-Anschluss. Zu Testzwecken.

Kabelloses Tablet

Tablet mit Kabellosinterface und grafischer Oberfläche.

Smart – Gerät

Smartphone mit Kabellosinterface und grafischer Oberfläche.

Allgemeines kabelgebundenes / kabelloses Gerät

Kabelgebundenes/Kabelloses Gerät mit integriertem FastEthernet-Port/ Kabellosinterface. Zur Traffic-Generierung.

Verbindungen (Tab. A.5)

Automatische Verbindung 

Wählt automatisch den passenden Kabeltyp zur Verbindung zweier Geräte.

Konsolenkabel 

Konsolenkabel zur Verbindung von PCs/Laptops mit Switches/Routern, um diese zu konfigurieren.

Standard RJ45-Kabel 

Standardkabel zur Verbindung von Geräten, welchen auf verschiedenen Schichten des OSI-Modells arbeiten.

RJ45-Crossoverkabel 

Standardkabel zur Verbindung von Geräten, welche auf der gleichen Schicht des OSI-Modells arbeiten.

Glasfaserkabel 

Kabel zur Verbindung von Geräten, basierend auf Glasfasertechnik.

Telefonkabel 

Kabel zur Anbindung an ein öffentliches Telefonnetz.

Koaxialkabel 

Kabel zur Verbindung von Geräten mittels Koaxialanschluss.

Serielles Kabel (DCE) 

Serielles Kabel, zur Verbindung von DC-Equipment.

Serielles Kabel (DTE) 

Serielles Kabel zur Verbindung von DT-Equipment.

Octalkabel 

Asynchrones 8-Port-Kabel. Eine Seite verfügt über einen High-Density-Anschluss, die andere über 8 RJ45-Anschlüsse.

Sonstige (Tab. A.6)

Hub	
Cisco-Hub mit 6 integrierten FastEthernet-Ports, sowie 4 Slots zur Erweiterung mit Interfacekarten.	
Repeater	
Cisco-Kabelrepeater mit 2 integrierten FastEthernet-Ports.	
Splitter	
Splitter für coaxiale Anbindung.	
Generic Cloud	
Repräsentiert eine Cloud zu Simulationszwecken. 10 Slots zur Erweiterung mit Interfacekarten.	
DSL Modem	
DSL Modem mit integriertem FastEthernet-Port und Telefonkabelanschluss. FastEthernet-Interface ist durch andere Inferfaces ersetzbar.	

Kabelmodem

Kabelmodem mit Coaxialanschluss und integriertem FastEthernet-Port. FastEthernet-Interface ist durch andere Interfaces ersetzbar.

Anlagen, Teil 3, Modulliste

Router-Interfacekarten (Tab. A.7)

HWIC-2T

Highspeed-WAN Interfacekarte. Fügt dem Gerät zwei serielle Ports hinzu.

HWIC-4ESW

Fügt dem Gerät 4 FastEthernet-Ports hinzu.

HWIC-8A

Fügt dem Gerät bis zu 8 asynchrone RS-232-Konsolen-Ports hinzu.

HWIC-AP-AG-B

Highspeed-WAN Interfacekarte mit integrierter Access-Point Funktion für Cisco 1800/2800/3800 Router. Unterstützt Single Band 802.11b/g bzw. Dual Band 802.11a/b/g

WIC-1AM

Fügt dem Gerät zwei Dual RJ-11 Modemanschlüsse für Standard Telefonverbindungen hinzu. Ein Port ist zur Verbindung mit der Standard-Telefonleitung gedacht, der andere wird zur Benutzung eines Standard-Analogtelefons verwendet (Modem im Idle-Modus).

WIC-1ENET

Fügt dem Gerät einen Ethernet-Port hinzu.

WIC-1T

Fügt dem Gerät einen seriellen Port, zur Anbindung an abgelegene Gebiete oder ältere Netzwerkgeräte (Alarmsysteme, Packet over SONET-Geräte), hinzu.

WIC-2AM

Fügt dem Gerät zwei Dual RJ-11 Anschlüsse für Standard Telefonverbindungen hinzu. Verfügt über zwei Modemports, um parallele Datenverbindungen zu ermöglichen.

WIC-2T

Fügt dem Gerät zwei serielle Ports hinzu. Beide Ports können individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-

WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

WIC-Cover

Schutzplatte für unbenutzte Interfacekartenslots.

Router-Modulkarten (Tab. A.8)

NM-1E

Verfügt über einen Ethernet-Port.

NM-1E2W

Verfügt über einen Ethernet-Port und zwei Steckplätze für Interfacekarten.

NM-1FE-FX

Verfügt über einen FastEthernet-Port zur Benutzung mit Glasfasertechnik.

NM-1FE-TX

Verfügt über einen FastEthernet-Port.

NM-1FE2W

Verfügt über einen FastEthernet-Port und zwei Steckplätze für Interfacekarten.

NM-2E2W

Verfügt über zwei Ethernet-Ports und zwei Steckplätze für Interfacekarten.

NM-2FE2W

Verfügt über zwei FastEthernet-Ports und zwei Steckplätze für Interfacekarten.

NM-2W

Verfügt über zwei Steckplätze für Interfacekarten.

NM-4A/S

Verfügt über 4 serielle Ports. Alle Ports können individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

NM-4E

Verfügt über 4 Ethernet-Ports.

NM-8A/S

Verfügt über 8 serielle Ports. Alle Ports können individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN,

dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

NM-8AM

Verfügt über 8 Modemanschlüsse für Standard Telefonverbindungen in öffentlichen oder privaten Telefonie Systemen.

NM-Cover

Schutzplatte für ungenutzte Modulkartenslots.

Generic-Router-Interfacekarten (Tab. A.9)

PT-ROUTER-NM-1AM

Fügt dem Gerät einen Dual RJ-11 Modemanschluss für Standard Telefonverbindungen hinzu.

PT-ROUTER-NM-1CE

Fügt dem Gerät einen Ethernet-Port hinzu.

PT-ROUTER-NM-1CFE

Fügt dem Gerät einen FastEthernet-Port hinzu.

PT-ROUTER-NM-1CGE

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PT-ROUTER-NM-1FFE

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-ROUTER-NM-1FGE

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-ROUTER-NM-1S

Fügt dem Gerät einen seriellen Port, zur Anbindung an abgelegene Gebiete oder ältere Netzwerkgeräte (Alarmsysteme, Packet over SONET-Geräte), hinzu.

PT-ROUTER-NM-1SS

Fügt dem Gerät einen seriellen Port hinzu. Der Port kann individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

Switch-Interfacekarten (Tab. A.10)

PT-SWITCH-NM-1CE 

Fügt dem Gerät einen Ethernet-Port hinzu.

PT-SWITCH-NM-1CFE 

Fügt dem Gerät einen FastEthernet-Port hinzu.

PT-SWITCH-NM-1CGE 

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PT-SWITCH-NM-1FFE 

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-SWITCH-NM-1FGE 

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

Hub-Interfacekarten (Tab. A.11)

PT-REPEATER-NM-1CE 

Fügt dem Gerät einen Ethernet-Port hinzu.

PT-REPEATER-NM-1CFE 

Fügt dem Gerät einen FastEthernet-Port hinzu.

PT-REPEATER-NM-1CGE 

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PT-REPEATER-NM-1FFE 

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-REPEATER-NM-1FGE 

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

Modem-Interfacekarten (Tab. A.12)

PT-MODEM-NM-1CE

Fügt dem Gerät einen Ethernet-Port hinzu.

PT-MODEM-NM-1CFE

Fügt dem Gerät einen FastEthernet-Port hinzu.

PT-MODEM-NM-1CGE

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

Cloud-Interfacekarten (Tab. A.13)

PT-CLOUD-NM-1AM

Fügt dem Gerät einen Dual RJ-11 Modemanschluss für Standard Telefonverbindungen hinzu.

PT-CLOUD-NM-1CE

Fügt dem Gerät einen Ethernet-Port hinzu.

PT-CLOUD-NM-1CFE

Fügt dem Gerät einen FastEthernet-Port hinzu.

PT-CLOUD-NM-1CGE

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PT-CLOUD-NM-1CX

Fügt dem Gerät einen Coaxialanschluss zur Anbindung eines Kabelmodems hinzu.

PT-CLOUD-NM-1FFE

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-CLOUD-NM-1FGE

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PT-CLOUD-NM-1S

Fügt dem Gerät einen seriellen Port hinzu. Der Port kann individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

PC/Server-Interfacekarten und -module (Tab. A.14)

Linksys-WMP300N

Fügt dem Gerät ein 2,4GHz Wireless-Interface hinzu.

PC-HOST-NM-1AM

Fügt dem Gerät einen Dual RJ-11 Modemanschluss für Standard Telefonverbindungen hinzu.

PC-HOST-NM-1CE

Fügt dem Gerät einen Ethernet-Port hinzu.

PC-HOST-NM-1CFE

Fügt dem Gerät einen FasttEthernet-Port hinzu.

PC-HOST-NM-1CGE

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PC-HOST-NM-1FFE

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PC-HOST-NM-1FGE

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PC-HOST-NM-1W

Fügt dem Gerät ein 2,4GHz Wireless-Interface hinzu.

PC-HOST-NM-1W-A

Fügt dem Gerät ein 5GHz Wireless-Interface hinzu.

PC-HEADPHONE

Schließt Kopfhörer an das Gerät an. Zu Testzwecken.

PC-MICROPHONE

Schließt ein Mikrofon an das Gerät an. Zu Testzwecken.

PC-CAMERA

Fügt dem Gerät einen seriellen Port hinzu. Der Port kann individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

PC-USB-HARD-DRIVE

Fügt dem Gerät einen seriellen Port hinzu. Der Port kann individuell synchron oder asynchron geschaltet werden. Unterstützung von Niedriggeschwindigkeits-WAN, dial-up Modem Verbindungen und Verbindungen zu Managementports anderer Geräte.

Laptop-Interfacekarten und -module (Tab. A.15)

Linksys-WMP300N 

Fügt dem Gerät ein 2,4GHz Wireless-Interface hinzu.

PC- LAPTOP-NM-1AM 

Fügt dem Gerät einen Dual RJ-11 Modemanschluss für Standard Telefonverbindungen hinzu.

PC- LAPTOP-NM-1CE 

Fügt dem Gerät einen Ethernet-Port hinzu.

PC-LAPTOP-NM-1CFE 

Fügt dem Gerät einen FasttEthernet-Port hinzu.

PC-LAPTOP-NM-1CGE 

Fügt dem Gerät einen GigabitEthernet-Port hinzu.

PC-LAPTOP-NM-1FFE 

Fügt dem Gerät einen FastEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PC-LAPTOP-NM-1FGE

Fügt dem Gerät einen GigabitEthernet-Port zur Benutzung mit Glasfasertechnik hinzu.

PC-LAPTOP-NM-1W

Fügt dem Gerät ein 2,4GHz Wireless-Interface hinzu.

PC-LAPTOP-NM-1W-A

Fügt dem Gerät ein 5GHz Wireless-Interface hinzu.

LAPTOP-HEADPHONE

Schließt Kopfhörer an das Gerät an. Zu Testzwecken.

LAPTOP-MICROPHONE

Schließt ein Mikrofon an das Gerät an. Zu Testzwecken.

LAPTOP-CAMERA

Schließt eine Kamera an das Gerät an. Zu Testzwecken.

LAPTOP-USB-HARD-DRIVE

Schließt eine Festplatte an das Gerät an. Zu Testzwecken.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 23.02.2016

Dustin Graupner